

Docket No.: 58799-096

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Customer Number: 20277
: :
Tatsuya FUJIYAMA, et al. : Confirmation Number:
: :
Serial No.: : Group Art Unit:
: :
Filed: September 30, 2003 : Examiner:
: :
For: SECURITY SPECIFICATION CREATION SUPPORT DEVICE AND METHOD OF
SECURITY SPECIFICATION CREATION SUPPORT

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

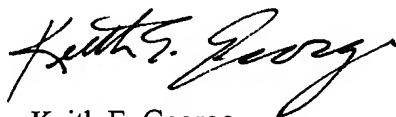
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-134706, filed May 13, 2003

cited in the Declaration of the present application. A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:prg
Facsimile: (202) 756-8087
Date: September 30, 2003

日本国特許庁
JAPAN PATENT OFFICE

58799-096
Fujiyama et al.
Sept. 30, 2003

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 5月13日

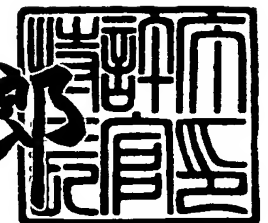
出願番号
Application Number: 特願2003-134706
[ST. 10/C]: [JP 2003-134706]

出願人
Applicant(s): 株式会社日立製作所

2003年 7月 9日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3055228

【書類名】 特許願

【整理番号】 HK14929000

【提出日】 平成15年 5月13日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 9/06

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 藤山 達也

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 永井 康彦

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 根本 繁幸

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100084032

【弁理士】

【氏名又は名称】 三品 岩男

【電話番号】 045(316)3711

【手数料の表示】

【予納台帳番号】 011992

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ仕様書作成支援装置、および、セキュリティ仕様書作成支援方法

【特許請求の範囲】**【請求項 1】**

情報ネットワークシステムに対するセキュリティ仕様書の作成を支援するセキュリティ仕様書作成支援装置であって、

既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースと、

前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受付ける定義情報受付手段と、

前記コンポーネント各々について、前記定義情報受付手段で受付けた当該コンポーネントの定義情報に基づいて、前記セキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定手段と、

所定のセキュリティ仕様書の雛形に、前記セキュリティ仕様書選定手段が検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受け付けるセキュリティ仕様書原案作成手段と、を有すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項 2】

請求項 1 記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書選定手段は、

前記コンポーネント各々について、前記セキュリティ仕様書事例データベースから再利用可能な事例を少なくとも 1 つ検出できた場合、検出できた事例の中から再利用する事例をユーザに選定させ、当該選定された事例を当該コンポーネントのセキュリティ仕様書原案とすると共に、当該原案の修正をユーザより受け付け、前記セキュリティ仕様書事例データベースから再利用可能な事例を検出できなかった場合、当該コンポーネントのセキュリティ仕様書原案をユーザより受け付けることで、前記コンポーネント各々のセキュリティ仕様書原案を作成し、

前記セキュリティ仕様書原案作成手段は、

前記セキュリティ仕様書の雛形に、前記コンポーネント各々のセキュリティ仕様書原案の内容を記述して、前記コンポジットセキュリティ仕様書原案を作成すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項 3】

請求項 2 記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書原案作成手段は、

前記コンポーネント各々のセキュリティ仕様書原案の記述の記載箇所を特定できるように、前記コンポジットセキュリティ仕様書原案を作成すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項 4】

請求項 1 記載のセキュリティ仕様書作成支援装置であって、

前記定義情報受付手段は、

前記情報ネットワークシステムを運用環境単位で分割することで得られるドメイン各々の定義情報と、前記ドメイン各々について、当該ドメインを装置単位で分割することで得られるサブシステム各々の定義情報と、前記サブシステム各々について、当該サブシステムをセキュリティ分析上の最小単位で分割することで得られるコンポーネント各々の定義情報とを、ユーザより受け付けること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項 5】

請求項 4 記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書原案作成手段は、

所定のセキュリティ仕様書の雛形に、前記ドメインあるいは前記サブシステムに属する前記コンポーネント各々のセキュリティ仕様書原案の内容を記述して、当該ドメインあるいは当該サブシステムのコンポジットセキュリティ仕様書原案を作成すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項 6】

請求項5記載のセキュリティ仕様書作成支援装置であって、
前記セキュリティ仕様書事例データベースには、
過去に作成されたドメインおよびサブシステムのコンポジットセキュリティ仕様書が事例として登録されており、
前記セキュリティ仕様書選定手段は、
前記ドメイン各々あるいは前記サブシステム各々について、前記定義情報受付手段で受付けた当該ドメインあるいは当該サブシステムの定義情報に基づいて、
前記セキュリティ仕様書事例データベースから再利用可能なドメインあるいはサブシステムのコンポジットセキュリティ仕様書の事例を検索すること
を特徴とするセキュリティ仕様書作成支援装置。

【請求項7】

請求項4記載のセキュリティ仕様書作成支援装置であって、
複数のサブシステム各々についてコンポーネント構成の典型パターンが事例として登録されたシステム構成事例データベースをさらに有し、
前記定義情報受付手段は、
ユーザより受付けたサブシステムの定義情報に基づいて、前記システム構成事例から当該サブシステムのコンポーネント構成の典型パターンを特定し、特定した典型パターンのコンポーネント構成が示すコンポーネント各々について、ユーザより定義情報を受付けること
を特徴とするセキュリティ仕様書作成支援装置。

【請求項8】

請求項4記載のセキュリティ仕様書作成支援装置であって、
前記定義情報受付手段により定義情報を受付けたドメイン、サブシステムおよびコンポーネントの各々を、前記情報ネットワークシステムにおける階層関係が識別可能なツリー構造で表示するツリー表示手段を有すること
を特徴とするセキュリティ仕様書作成支援装置。

【請求項9】

請求項8記載のセキュリティ仕様書作成支援装置であって、
前記ツリー表示手段は、

同一のサブシステムを構成するコンポーネントの各々を、前記サブシステムにおける階層関係が識別可能なレイヤ構造で表示すること
を特徴とするセキュリティ仕様書作成支援装置。

【請求項 10】

請求項 8 記載のセキュリティ仕様書作成支援装置であって、
前記ツリー表示手段は、
コンポーネント各々を、前記セキュリティ仕様書選定手段による事例の検出の有無が識別可能に表示すること
を特徴とするセキュリティ仕様書作成支援装置。

【請求項 11】

請求項 1 記載のセキュリティ仕様書作成支援装置であって、
前記セキュリティ仕様書事例データベースは、ネットワークを介して、前記セキュリティ仕様書選定手段から離れて配置されていること
を特徴とするセキュリティ仕様書作成支援装置。

【請求項 12】

情報ネットワークシステムに対するセキュリティ仕様書の作成を支援するためのコンピュータで読取り可能なプログラムであって、

前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受け付ける定義情報受付手段と、

前記コンポーネント各々について、前記定義情報受付手段で受け付けた当該コンポーネントの定義情報に基づいて、既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定手段と、

所定のセキュリティ仕様書の雛形に、前記セキュリティ仕様書選定手段が検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受け付けるセキュリティ仕様書原案作成手段として、前記コンピュータを機能させることを特徴とするコンピュータで読取り可能なプログラム。

【請求項 13】

コンピュータを用いて情報ネットワークシステムに対するセキュリティ仕様書の作成を支援するセキュリティ仕様書作成支援方法であって、

前記コンピュータあるいはネットワークを介して前記コンピュータに接続された他のコンピュータの記憶装置には、既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースが格納されており、

前記コンピュータの演算装置は、

前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受け付ける定義情報受付ステップと、

前記コンポーネント各々について、前記定義情報受付ステップで受け付けた当該コンポーネントの定義情報に基づいて、前記セキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定ステップと、

所定のセキュリティ仕様書の雛形に、前記セキュリティ仕様書選定ステップで検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受け付けるセキュリティ仕様書原案作成ステップと、を行うこと

を特徴とするセキュリティ仕様書作成支援方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、セキュリティ仕様書、特に、国際セキュリティ評価基準 ISO 15408 に従ったセキュリティ仕様書の作成を支援する技術に関する。

【0002】

【従来の技術】

IT (Information Technology) 製品のセキュリティ機能の設計・評価に関する基準として、国際セキュリティ評価基準 ISO/IEC 15408 (CC: Common Criteria) がある。この ISO 15408 に準拠した製品の開発を行い、その評価・認証を取得するためには、ISO 15408 特有のセキュリティ要求仕様書 (PP: Protection Profile) またはセキュリティ設計仕様書 (ST: Security Target) を作成することが必須となっている。以下では、セキュリティ要求

仕様書およびセキュリティ設計仕様書を、セキュリティ仕様書と呼ぶこととする。これらのセキュリティ仕様書を作成するには、セキュリティ全般およびISO 15408に関する専門知識は勿論のこと、対象製品に固有の脅威や対策事例に関する豊富な知識や、どの脅威に対してどの対策が有効であるかといったセキュリティに関するノウハウや、リスク分析等の分析業に関わる専門技術が必要であるという問題がある。また、リスク分析等の分析作業の実施には、脅威や対策等に対して抜け漏れのない洗い出しや、対策のための適切なセキュリティ要件の選択などが必要であり、このため、膨大な時間を要するという問題もある。

【0003】

これらの問題に対応するISO 15408準拠のセキュリティ設計支援ツールとして、米国のセキュリティ認証機関であるNIAP (The National Information Assurance Partnership) によるCC Tool Box (TM) (商標権者: National Security Agency)や、非特許文献1や、特許文献1に記載のものがある。

【0004】

CC Tool Box (TM)や非特許文献1に記載のセキュリティ設計支援ツールは、セキュリティ仕様書に記載する脅威やセキュリティ対策方針等の各種定義情報の事例を事前登録したデータベースを用意し、そのデータベースからユーザが直接選択した定義情報や、提示された質問にユーザが答えることによってデータベースから抽出された定義情報を、セキュリティ仕様書の所定箇所に自動的に記載する。これにより、定義情報をユーザが自ら考案する負担を低減しつつ、所定形式に沿ったセキュリティ仕様書を自動作成することができる。

【0005】

また、特許文献1に記載のセキュリティ設計支援ツールは、評価・認証後に登録機関によって管理される認証済みのセキュリティ仕様書や、過去に作成した既存のセキュリティ仕様書をデータベース化し、脅威等の各種定義情報の事例を個別に再利用できるようにするだけでなく、認証済みのセキュリティ仕様書の定義情報一式も再利用できるようにしている。このようにすることで、仕様書作成時のリスク分析等の作業負担を低減することができる。

【0006】

【非特許文献1】

「セキュリティ設計評価支援ツール(V3.0) 利用者マニュアル」、情報処理振興事業協会セキュリティセンター、2002年5月、p.2-69

【特許文献1】

特開 2001-222420号公報

【0007】**【発明が解決しようとする課題】**

上述した従来のセキュリティ設計支援ツールは、個々のIT製品に対するセキュリティ仕様書の作成を支援することを前提にしている。複数のIT製品を構成要素とする情報ネットワークシステムでは、既存のIT製品と新規開発のIT製品とが混在している場合もある。上述した従来のセキュリティ設計支援ツールは、このような情報ネットワークシステムに対するセキュリティ仕様書の作成を支援することについて考慮されていない。

【0008】

本発明は上記事情に鑑みてなされたものであり、本発明の目的は、複数のIT製品で構成される情報ネットワークシステムに対するセキュリティ仕様書の作成を支援することにある。

【0009】**【課題を解決するための手段】**

上記課題を解決するために、本発明は、情報ネットワークシステムを構成する各コンポーネントの定義情報をユーザより受付ける。次に、コンポーネント各々について、既存のセキュリティ仕様書を蓄積したデータベースに再利用可能なセキュリティ仕様書が存在するか否かを調べ、存在するならばこれを特定する。それから、予め用意してあるセキュリティ仕様書の雛形に前記特定したセキュリティ仕様書各々の内容を反映して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書の原案を自動生成し、ユーザに提示する。そして、ユーザよりコンポジットセキュリティ仕様書の原案の修正を受付ける。このようにすることで、専門知識・技術やノウハウをもたないユーザが情報ネットワークシステムのセキュリティ仕様書原案を作成することを支援する。

【0010】

例えば、本発明のセキュリティ仕様書作成支援装置は、既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースと、前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受付ける定義情報受付手段と、前記コンポーネント各々について、前記定義情報受付手段で受付けた当該コンポーネントの定義情報に基づいて、前記セキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定手段と、所定のセキュリティ仕様書の雛形に、前記セキュリティ仕様書選定手段が検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受付けるセキュリティ仕様書原案作成手段と、を有する。

【0011】

ここで、前記セキュリティ仕様書選定手段は、前記コンポーネント各々について、前記セキュリティ仕様書事例データベースから再利用可能な事例を少なくとも1つ検出できた場合、検出できた事例のなかから再利用する事例をユーザに選定させ、当該選定された事例を当該コンポーネントのセキュリティ仕様書原案とすると共に、当該原案の修正をユーザより受け、前記セキュリティ仕様書事例データベースから再利用可能な事例を検出できなかった場合、当該コンポーネントのセキュリティ仕様書原案をユーザより受け付けることで、前記コンポーネント各々のセキュリティ仕様書原案を作成してもよい。また、前記セキュリティ仕様書原案作成手段は、前記セキュリティ仕様書の雛形に、前記コンポーネント各々のセキュリティ仕様書原案の内容を記述して、前記コンポジットセキュリティ仕様書原案を作成してもよい。

【0012】

また、前記定義情報受付手段は、前記情報ネットワークシステムを運用環境単位で分割することで得られるドメイン各々の定義情報と、前記ドメイン各々について、当該ドメインを装置単位で分割することで得られるサブシステム各々の定義情報と、前記サブシステム各々について、当該サブシステムをセキュリティ分析上の最小単位で分割することで得られるコンポーネント各々の定義情報とを、

ユーザより受付けるようにしてもよい。

【0013】

また、前記セキュリティ仕様書事例データベースは、ネットワークを介して、前記セキュリティ仕様書選定手段から離れて配置されているようにしてもよい。

【0014】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【0015】

図1は、本発明の一実施形態が適用されたセキュリティ仕様書作成支援装置11により、コンポジットセキュリティ仕様書原案の作成対象である情報ネットワークシステム（設計対象システムと呼ぶ）16に対するコンポジットセキュリティ仕様書原案が作成されるまでの大まかな処理の流れ（原理）を示している。

【0016】

本実施形態のセキュリティ仕様書作成支援装置11は、設計対象システム16のシステム構成等のシステム計画・設計段階における情報に基づいて、再利用可能な既存のセキュリティ仕様書を選定し、これらを利用して設計対象システムに対するコンポジットセキュリティ仕様書の作成を支援する。

【0017】

図示するように、セキュリティ仕様書作成支援装置11は、設計対象システム16を定義するシステム構成定義機能111と、セキュリティ仕様書の事例が登録された仕様書事例DB（データベース）12からコンポジットセキュリティ仕様書原案に再利用可能なセキュリティ仕様書を選定するセキュリティ仕様書選定機能112と、設計対象システムに対するコンポジットセキュリティ仕様書の原案を自動作成するセキュリティ仕様書原案作成機能113と、を有する。

【0018】

システム構成定義機能111は、例えばGUI（Graphical User Interface）を介してユーザより設計対象システム16の階層構造を示す定義情報を受付ける。具体的には、ユーザの指示に従い、設計対象システム16を、ドメイン（例えば地理的条件や会社の組織構成といった運用環境単位で分類される構成要素）の

階層 161、サブシステム（例えば IT 製品、ネットワークといった装置単位で分類される構成要素）の階層 162、および、コンポーネント（ソフト部品、ハード部品といったセキュリティ分析上の最小単位で分類される構成要素）の階層 163 の 3 つ階層に分ける。そして、階層 161～163 毎に、構成要素の定義情報をユーザより受付ける。ドメインの階層 161 ならば、各ドメイン 1～L の運用方針および他ドメインとのインターフェースに関するドメイン間対応情報を各ドメイン 1～L の定義情報として受付ける。サブシステムの階層 162 ならば、各サブシステム 1～M の所属ドメインおよびサブシステム間対応情報を各サブシステム 1～M の定義情報として受付ける。そして、コンポーネントの階層 163 ならば、各コンポーネント 1～N の所属サブシステム、コンポーネント固有情報およびコンポーネント間対応情報を各コンポーネント 1～N の定義情報として受付ける。

【0019】

仕様書事例 DB12 には、既存のセキュリティ仕様書（認証済みセキュリティ仕様書、過去に作成したセキュリティ仕様書、業界標準や顧客の要件を記述したセキュリティ仕様書等）が事例として登録されている。セキュリティ仕様書選定機能 112 は、コンポーネント各々について、定義情報と適合する事例を仕様書事例 DB12 から検索する。そして、コンポーネント各々について、ユーザよりの指示に従い、検索した事例の中からコンポジットセキュリティ仕様書原案に再利用可能な既存のセキュリティ仕様書 17 を選定する。

【0020】

セキュリティ仕様書原案作成機能 113 は、コンポーネント各々について、当該コンポーネントに対して選定された既存のセキュリティ仕様書 17 を、当該コンポーネントに対するセキュリティ仕様書原案 19 とする。このとき、既存のセキュリティ仕様書 17 が選定されなかったコンポーネントについては、ユーザが新規作成したセキュリティ仕様書を、当該コンポーネントに対するセキュリティ仕様書原案 19 とする。また、予め用意してあるセキュリティ仕様書の雛形に、各コンポーネントのセキュリティ仕様書原案 19 各々の内容を反映する。これより、コンポジットセキュリティ仕様書原案 18 および各コンポーネントのセキュ

リティ仕様書原案 19 を有するシステムセキュリティ仕様書原案 13 を自動生成する。そして、システムセキュリティ仕様書原案 13 を、例えば GUI を介してユーザに提示して編集を受け付ける。

【0021】

図 2 は、設計対象システムの一例を示す図である。

【0022】

図 2 に示す設計対象システムの例は、社員の勤休管理を行う情報ネットワークシステム（勤休管理システム）である。この勤休管理システムを構成する IT 製品は、本社拠点区域 21 に存在するものと、支社拠点区域 22 に存在するものとに分類することができる。

【0023】

本社拠点区域 21 に属する IT 製品としては、本社ビル 215 内に存在する一般利用者端末 211、本社ビル 215 の情報機器室 216 内に存在する勤休管理サーバ機器 212 および社員情報 DB 213、および、本社拠点区域 21 内の各 IT 製品を接続する拠点内ネットワーク 214 がある。一方、支社拠点区域 22 に属する IT 製品としては、支社ビル 223 内に存在する一般利用者端末 221、および、支社拠点区域 22 内の各 IT 製品を接続する拠点内ネットワーク 222 がある。そして、拠点内ネットワーク 214 および拠点内ネットワーク 222 は拠点間ネットワークであるインターネット 23 を介して相互接続されている。

【0024】

また、一般利用者端末 211、221 を構成する部品としては、AT 互換ハードウェア 2114、ネットワークカード 2115、AT 互換ハードウェア 2114 上で動作する端末 OS 2113、端末 OS 2113 上で動作する勤休入力用ブラウザ 2111、および、端末 OS 2113 上で動作する通知受信用メーラ 2112 がある。一方、勤休管理サーバ機器 212 を構成する部品としては、AT 互換ハードウェア 2125、ネットワークカード 2126、AT 互換ハードウェア 2125 上で動作するサーバ OS 2124、サーバ OS 2124 上で動作する DBMS (DataBase Management System) 2123、DBMS 2123 上で動作する勤休管理用サーバ 2121、および、DBMS 2123 上で動作するメールサ

ーバ 2122 がある。

【0025】

以上のような構成を有する勤休管理システムにおいて、一般社員は一般利用端末 211、221 の勤休入力用ブラウザ 2111 を使用して勤休管理サーバ 212 にアクセスし、勤休情報を登録・参照することができる。また、一般利用端末 211、221 の通知受信用メーラ 2112 により、登録情報の修正依頼等の通知を受信することができる。

【0026】

図 3 は、セキュリティ仕様書作成支援装置 11 が作成を支援するセキュリティ仕様書を説明するための図である。

【0027】

ここで、図 3 (A) は、国際セキュリティ評価基準 ISO 15408 に従ったセキュリティ仕様書 (PP/ST) の構成例 31 および各種定義情報の記述例 33 を示している。図示するように、ISO 15408 準拠のセキュリティ仕様書には、仕様書タイトル 311、対象製品名 312、TOE (Target of Evaluation) 313、前提条件 331、組織のセキュリティ方針 332、および、評価保証レベル 333 を含む複数の所定の項目が設けられている。ISO 15408 準拠のセキュリティ仕様書では、目次構成および各目次におかる記述内容が規定されている。このため、目的の情報がどの目次にあるかを特定できれば、セキュリティ仕様書から目的の情報を適切に参照したり抽出したりすることができる。

【0028】

図 3 (B) は、コンポジットセキュリティ仕様書の一例 35 を示している。図示するように、コンポジットセキュリティ仕様書は、国際セキュリティ評価基準 ISO 15408 に準拠している。上述したように、本実施形態のセキュリティ仕様書作成支援装置 11 が作成を支援するシステムセキュリティ仕様書原案 13 は、設計対象システム 16 を構成する各コンポーネントのセキュリティ仕様書原案 19 および設計対象システムのコンポジットセキュリティ仕様書原案 18 を備えて構成される。そして、コンポジットセキュリティ仕様書原案 18 は、設計対象システムのセキュリティ環境記述に該当する記述のあるコンポーネントのセキ

セキュリティ仕様書原案 19 や、設計対象システムのセキュリティ対策方針、セキュリティ要件およびセキュリティ機能を実現するコンポーネントのセキュリティ仕様書原案 19 の記述内容が参照（反映）されるように自動生成される。このようにして、システム全体について抜け漏れなく記述するものである。コンポジットセキュリティ仕様書の一例 35 では、各コンポーネントのセキュリティ仕様書の記述内容が参照されている部分（下線 35 1 が引いてある部分）を特定可能なように、コンポジットセキュリティ仕様書が作成されている。

【0029】

図 4 は、本実施形態のセキュリティ仕様書作成支援装置 11 の概略構成図である。図示するように、本実施形態のセキュリティ仕様書作成支援装置 11 は、CPU 51 と、メモリ 52 と、HDD 等の外部記憶装置 54 と、LCD、CRT 等の表示装置 56 およびキーボード、マウス等の入力装置 57 を介してユーザに情報を提示したり、ユーザから情報を受付けたりする端末入出力装置 52 と、ネットワークを介して通信を行うためのネットワーク IF（インターフェース）装置 58 と、CD-ROM、DVD-ROM、MO、フレキシブルディスク等の可搬記憶媒体の読み込み・書き出しを制御する可搬記憶媒体入出力装置 59 と、これらの各装置を相互接続するバス 53 と、を備えた通常のコンピュータシステムにおいて、CPU 51 がメモリ 55 にロードされた通信制御 PG（プログラム）541 およびセキュリティ仕様書作成支援 PG 542 を実行することで実現される。

【0030】

ここで、通信制御 PG 541 は、CPU 51 がネットワーク IF 装置 58 を介してネットワークに接続された他のネットワーク端末と通信を行うためのプログラムである。また、セキュリティ仕様書作成支援 PG 542 は、図 1 に示すシステム構成定義機能 111、セキュリティ仕様書選定機能 112 およびセキュリティ仕様書原案作成機能 113 を実現するためのプログラムである。本実施形態では、セキュリティ仕様書作成支援 PG 542 を、システム構成定義機能 111 を実現するためのシステム構成定義 PG 5421、セキュリティ仕様書選定機能 112 を実現するためのセキュリティ仕様書選定 PG 5422、および、セキュリティ仕様書原案作成機能 113 を実現するためのセキュリティ仕様書原案作成 P

G5423の、3つのプログラムを含めて構成している。通信制御PG541およびセキュリティ仕様書作成支援PG542は、例えば外部記憶装置54あるいは可搬記憶媒体591に予め格納される。そして、外部記憶装置54から、あるいは、可搬記憶媒体入出力装置59を介して可搬記憶媒体59から、メモリ55上にロードされる。

【0031】

外部記憶装置54あるいは可搬記憶媒体591には、各種DB543～545が格納される。セキュリティ仕様書事例DB543には、認証済みセキュリティ仕様書、過去に作成したセキュリティ仕様書、および、業界標準や顧客の要件を記述したセキュリティ仕様書を含む既存のセキュリティ仕様書が事例として登録されており、図1に示す仕様書事例DB12に相当する。

【0032】

図5は、セキュリティ仕様書事例DB543のデータ管理の仕組みを説明するための図である。図示するように、セキュリティ仕様書事例DB543は、既存のセキュリティ仕様書の事例が、コンポーネントの種類を示すカテゴリ5431および同一種類のコンポーネントの形式を示すタイプ5432をキーとして検索できるようにデータベース化されている。

【0033】

システム構成事例DB544には、情報ネットワークシステムを構成する各サブシステムの典型的なシステム展開パターンがシステム構成事例として登録されている。ここで、システム展開パターンとはサブシステムのツリー構成を特定するためのデータであり、システム展開パターンによりサブシステムを構成する各コンポーネントを特定できる。

【0034】

図6は、システム構成事例DB544の登録例を示す図である。図示するように、本実施形態では、システム展開パターン5441をタグ形式で記述している。ここで、＜サブシステム＞タグ5443aおよび＜/サブシステム＞5443bで囲まれた領域に、サブシステムの名称および該システムを構成する各コンポーネントの情報が記述され、＜サブシステム＞タグ5443aの次に位置する2

つのタグ<要素名>、</要素名>で囲まれた領域 5 4 4 6 に、サブシステムのタイプが記述される。また、<コンポーネント>タグ 5 4 4 4 a および</コンポーネント> 5 4 4 4 b で囲まれた領域に、コンポーネントの名称および該コンポーネントの定義や仕様書に関する情報が記述され、<コンポーネント>タグ 5 4 4 4 a の次に位置する 2 つのタグ<要素名>、</要素名>で囲まれた領域 5 4 4 7 に、コンポーネントのタイプが記述される。システム構成例 DB 5 4 4 は、サブシステムのタイプを検索キーとして、所望のサブシステムのシステム展開パターン 5 4 4 1 を検索できるようにデータベース化されている。

【0035】

運用環境事例 DB 5 4 5 には、過去にシステムセキュリティ仕様書が作成された情報ネットワークシステムの各サブシステムの運用環境パターンが運用環境事例として登録されている。ここで、運用環境パターンとは、サブシステムのシステム展開パターンに、該システムの各コンポーネントに適用した運用方針や前提条件が記述されて構成されたものである。

【0036】

図 7 は、運用環境事例 DB 5 4 5 の登録例を示す図である。図示するように、運用環境パターン 5 4 5 1 は、図 6 に示すシステム展開パターン 5 4 4 1 において、サブシステムおよびコンポーネント各々の記述領域に、対応する構成要素に適用した運用方針や前提条件を記述するための領域（2 つのタグ<運用>、</運用>で囲まれた領域） 5 4 5 2 が設けられて構成されている。運用環境事例 DB 5 4 5 も、システム構成例 DB 5 4 4 と同様に、サブシステムのタイプを検索キーとして、所望のサブシステムの運用環境パターン 5 4 5 1 を検索できるようにデータベース化されている。

【0037】

また、メモリ 5 5 には、CPU 5 1 がメモリ 5 5 にロードされたセキュリティ仕様書作成支援 PG 5 4 2 を実行することにより、運用環境事例 DB 5 4 5 から読み出した運用環境事例を一時格納するための運用環境事例格納領域 5 5 1、システム構成事例 DB 5 4 4 から読み出したシステム構成事例を一時格納するためのシステム構成事例格納領域 5 5 2、セキュリティ仕様書事例 DB 5 4 3 から読

み出したセキュリティ仕様書事例を一時格納するためのセキュリティ仕様書事例格納領域553、設計対象システムの定義情報を一時格納するための設計対象システム定義情報格納領域554、および、設計対象システムのセキュリティ仕様書原案を一時格納するためのセキュリティ仕様書原案格納領域555が、それぞれ形成される。

【0038】

図8は、本実施形態のセキュリティ仕様書作成支援装置11の動作フローを説明するための図である。

【0039】

まず、システム構成定義PG5421は、端末入力装置52を介して、設計対象システムの階層構造を示す定義情報を、ユーザより対話的に受付ける。そして、設計対象システムの定義情報を設計対象システム定義情報格納領域554に格納する(S711)。

【0040】

次に、セキュリティ仕様書選定PG5422は、設計対象システム定義情報格納領域554に格納された、設計対象システムの定義情報により特定されるコンポーネントの中からコンポーネントを1つ抽出し、これを注目コンポーネントとする。そして、注目コンポーネントの定義情報(カテゴリ5431、タイプ5432)と適合するセキュリティ仕様書の事例を検出する。そして、ユーザの指示に従い、検出した事例の中から、注目コンポーネントに対して再利用可能なセキュリティ仕様書の事例(例えば所属ドメインの運用方針と適合するセキュリティ仕様書の事例)を選択する(S712)。

【0041】

次に、セキュリティ仕様書選定PG5422は、注目コンポーネントに対して再利用可能なセキュリティ仕様書の事例を選定できた場合(S713でYes)、これをセキュリティ仕様書事例DB543から読み出してセキュリティ仕様書事例格納領域553に格納する。次に、セキュリティ仕様書原案作成PG5423は、セキュリティ仕様書事例格納領域553に格納されたセキュリティ仕様書の事例を、端末入力装置52を介して、ユーザに提示し、その修正を受付ける

。これにより、注目コンポーネントに対するセキュリティ仕様書原案が作成される。そして、ユーザの登録指示に従い、注目コンポーネントに対するセキュリティ仕様書原案を、それが既存のセキュリティ仕様書の事例をベースにしていることが分かるようにして、セキュリティ仕様書原案格納領域555に格納する（S714）。それからS716に移行する。

【0042】

一方、セキュリティ仕様書選定PG5422が注目コンポーネントに対して再利用可能なセキュリティ仕様書の事例を選定できなかった場合（S713でNo）、セキュリティ仕様書原案作成PG5423は、端末入力装置52を介してユーザより、注目コンポーネントに対するセキュリティ仕様書原案を新規に受け付ける。そして、ユーザの登録指示に従い、注目コンポーネントに対するセキュリティ仕様書原案を、それが新規作成されたものであることが分かるようにして、セキュリティ仕様書原案格納領域555に格納する（S715）。それからS716に移行する。

【0043】

次に、S716において、セキュリティ仕様書選定PG5422は、設計対象システムの定義情報により特定されるコンポーネント中に、注目コンポーネントとして未抽出のコンポーネントがあるか否かを調べる。そして、未抽出のコンポーネントがあるならば（S716でNo）、S712に戻る。

【0044】

一方、設計対象システムの定義情報により特定される全てのコンポーネントが注目コンポーネントとして抽出された場合、つまり、設計対象システムの定義情報により特定される全てのコンポーネントに対するセキュリティ仕様書原案がセキュリティ仕様書原案格納領域555に格納された場合（S716でYes）、セキュリティ仕様書原案作成PG5423は、予め用意してあるセキュリティ仕様書の雛形に、各コンポーネントのセキュリティ仕様書原案の内容を反映させて、設計対象システムに対するコンポジットセキュリティ仕様書原案を自動作成する（S717）。

【0045】

具体的には、ISO15408準拠セキュリティ仕様書のある目次について、当該目次における記述内容を、各コンポーネントのセキュリティ仕様書原案から抽出し、これらを予め用意してあるセキュリティ仕様書の雛形における当該目次の内容記述部分に追加する。この際、追加した記述内容の参照元（コンポーネントのセキュリティ仕様書原案）へのリンク情報を追加する。以上の処理を、ISO15408準拠セキュリティ仕様書の全ての目次に対して繰り返し行うことにより、各コンポーネントのセキュリティ仕様書原案の内容が反映された、設計対象システムに対するコンポジットセキュリティ仕様書原案を自動作成する。

【0046】

次に、セキュリティ仕様書原案作成PG5423は、自動作成した設計対象システムに対するコンポジットセキュリティ仕様書原案を、端末入力装置52を介して、ユーザに提示し、その修正を受付ける。そして、ユーザの登録指示に従い、設計対象システムに対するコンポジットセキュリティ仕様書原案を、セキュリティ仕様書原案格納領域555に格納する（S718）。

【0047】

セキュリティ仕様書原案格納領域555に格納されたコンポジットセキュリティ仕様書原案および各コンポーネントのセキュリティ仕様書原案は、設計対象システムのシステムセキュリティ仕様書原案として、端末入出力装置52を介してユーザに提示されたり、外部記憶装置54や可搬記憶媒体入出力装置59に装着された可搬記憶媒体591に記憶されたり、ネットワークIF装置58を介してネットワークへ送信されたりする。

【0048】

図9は、図8のS711での処理（設計対象システムの定義情報の受付・登録）の詳細なフローを示す図である。

【0049】

先ず、システム構成定義PG5421は、端末入力装置52を介してユーザより、設計対象システムを構成する各ドメインの設定を受付ける（S7111）。ユーザは、例えば地理的条件や会社の組織構成などに基づいて、設計対象システムを、共通の運用方針が適用されるサブシステムのグループである複数のドメ

インに分割する。そして、各ドメインの設定をセキュリティ仕様書作成支援装置 11 に入力する。

【0050】

次に、システム構成定義 PG 5421 は、端末入力装置 52 を介してユーザより、上記の S 7111 で受付けた各ドメインについて、運用方針を含むドメイン固有情報および他ドメインとのインターフェースに関するドメイン間対応情報を、ドメインの定義情報として受付ける (S 7112)。

【0051】

次に、システム構成定義 PG 5421 は、端末入力装置 52 を介してユーザより、ドメイン各々について当該ドメインに属するサブシステムの設定を受付ける (S 7113)。ユーザは、ドメイン各々について、当該ドメインに属する IT 製品、ネットワークインフラ等の個々のサブシステムを特定し、特定したサブシステム各々の設定をセキュリティ仕様書作成支援装置 11 に入力する。

【0052】

次に、システム構成定義 PG 5421 は、端末入力装置 52 を介してユーザより、上記の S 7113 で受付けた各サブシステムについて、サブシステム固有情報および他サブシステムとのインターフェースに関するサブシステム間対応情報を、サブシステムの定義情報として受付ける (S 7114)。

【0053】

次に、システム構成定義 PG 5421 は、端末入力装置 52 を介してユーザより、サブシステム各々について当該サブシステムを構成するコンポーネントの設定を受付ける (S 7115)。ユーザは、サブシステム各々について、当該サブシステムを構成するソフト部品、ハード部品等の個々のコンポーネントを特定し、特定したコンポーネント各々の設定をセキュリティ仕様書作成支援装置 11 に入力する。

【0054】

次に、システム構成定義 PG 5421 は、端末入力装置 52 を介してユーザより、上記の S 7115 で受付けた各コンポーネントについて、コンポーネント固有情報および他コンポーネントとのインターフェースに関するコンポーネント

間対応情報を、コンポーネントの定義情報として受付ける（S7116）。

【0055】

以上のようにして、ドメイン、サブシステムおよびコンポーネントの定義情報を受付けたならば、システム構成定義PG5421は、これらの定義情報を設計対象システムの階層構造を示す定義情報として、設計対象システム定義情報格納領域554に格納する。

【0056】

図10は、システム構成定義PG5421が表示装置56に表示する作業画面のメニューバーの一例を示す図である。先ず、図10を用いて、図8のS711（設計対象システムの定義情報の受付、図9に示すフロー）における操作手順と画面構成を説明する。

【0057】

システム構成定義PG5421は、図10（A）に示すように、初期画面として仕様書編集画面91を表示する。入力装置57を介してカーソル（不図示）が操作されて、ユーザにより、メニューバーの項目「ツール」911から項目「TOE定義支援」9111が選択されると、設計対象システム定義情報格納領域554に格納されている設計対象システムの定義情報によって特定されるシステム展開ツリー（設計対象システムの階層構造）を表示するTOE定義画面92を、端末入出力装置52を介して表示装置56に表示する。なお、このTOE定義画面92を閉じる場合、図10（B）に示すように、ユーザはメニューバーの項目「ファイル」921から項目「閉じる」9211を選択すればよい。

【0058】

図11は、システム構成定義PG5421が表示装置56に表示するTOE定義画面92の一例を示している。この例では、図8に示すフローが実行されて、図2に示す勤休管理システムの定義情報が設計対象システム定義情報格納領域554に格納され、また、勤休管理システムのシステムセキュリティ仕様書原案がセキュリティ仕様書原案格納領域555に格納された状態にて、項目「TOE定義支援」9111が選択された場合を示している。

【0059】

システム構成定義PG5421は、表示枠924に、設計対象システム定義情報格納領域554に格納されている設計対象システムの定義情報により特定されるシステム展開ツリーを表示する。なお、設計対象システム定義情報格納領域554に設計対象システムの定義情報が格納されていない状態、つまり、これから設計対象システムの定義情報を受付ける状態では、表示枠924には何も表示されない。

【0060】

図11において、四角マークのノード9241～9243がドメインである。図2に示す勤休管理システムの場合、「本社拠点区域」ドメイン9241、「支社拠点区域」ドメイン9242、および、「拠点間ネットワーク」ドメイン9243の3つのドメインに分けることができる。なお、ドメインの追加は、図10(C)に示すように、入力装置57を介してカーソル(不図示)を操作し、TOE定義画面92において、メニューバーの項目「編集」922から項目「要素の追加」9222を選択し、さらに項目「ドメイン」9223を選択することで行う。これにより、システム構成定義PG5421は、「TOE」ノード9240に接続する四角マークの新たなノードを追加表示する(図9のS7111)。

【0061】

また、図11において、三角マークのノード9244、9245がサブシステムである。図2に示す勤休管理システムの場合、例えば「本社拠点区域」ドメイン9241には、「一般利用者端末」サブシステム9244および「勤休管理サーバ」サブシステム9245が属している。なお、サブシステムの追加は、図10(C)に示すように、入力装置57を介してカーソル(不図示)を操作し、TOE定義画面92において、メニューバーの項目「編集」922から項目「要素の追加」9222を選択し、さらに項目「サブシステム」9224を選択すると共に、所望のドメインのノードを指定することで行う。これにより、システム構成定義PG5421は、所望のドメインのノードに接続する三角マークの新たなノードを追加表示する(図9のS7113)。

【0062】

また、図11において、丸マークのノード9246～9256がコンポーネン

トである。図2に示す勤休管理システムの場合、例えば「一般利用者端末」サブシステム9244には、「アプリ層」コンポーネント9246、「勤休入力用ブラウザ」コンポーネント9249、「通知受信用メール」コンポーネント9250、「OS層」コンポーネント9247、「端末OS」9251、「ハードウェア層」コンポーネント9248、「AT互換ハードウェア」コンポーネント9252、「ネットワークカード」9253が属している。なお、コンポーネントの追加は、図10(C)に示すように、入力装置57を介してカーソル（不図示）を操作し、TOE定義画面92において、メニューバーの項目「編集」922から項目「要素の追加」9222を選択し、さらに項目「コンポーネント」9225を選択すると共に、所望のサブシステムあるいはコンポーネントのノードを指定することで行う。これにより、システム構成定義PG5421は、所望のサブシステムあるいはコンポーネントのノードに接続する丸マークの新たなノードを追加表示する（図9のS7115）。

【0063】

ここで、コンポーネントのノードを、サブシステムのノードみならず、他のコンポーネントのノードにも接続できるようにすることで、同一レイヤのコンポーネントを水平方向に展開する方法で表示することができる。これにより、ネットワーク接続関係にあるような水平分散する要素群（ドメイン、サブシステム）と、IT製品のレイヤ構造のような垂直展開する要素群（コンポーネント）との両方を識別することができる。

【0064】

また、システム構成定義PG5421は、表示枠926に、表示枠924に表示されているシステム展開ツリーから、ユーザがカーソル（不図示）を操作して選択したノードの定義情報を表示する。図11に示す例では、「勤休入力用ブラウザ」コンポーネント9249が選択され、その定義情報が表示枠926に表示されている。なお、設計対象システム定義情報格納領域554に、選択されたノードの定義情報が格納されていない状態、つまり、これから当該ノードの定義情報を受付ける状態では、表示枠926には何も表示されない。

【0065】

また、図10(C)に示すように、ユーザがカーソル(不図示)を操作して表示枠924に表示されているドメインのノードを指定し、TOE定義画面92において、メニューバーの項目「編集」922から項目「定義情報の設定」9221を選択すると、システム構成定義PG5421は、設計対象システム定義情報格納領域554に格納されている当該ドメインの定義情報を表示すると共に当該ドメインの定義情報の修正を受付けるためのドメイン定義画面93を、端末入出力装置52を介して表示装置56に表示する。

【0066】

図12は、システム構成定義PG5421が表示装置56に表示するドメイン定義画面93の一例を示している。この例では、図11において「本社拠点区域」ドメイン9241が指定された場合であって、「本社拠点区域」ドメイン9241の定義情報が既に設計対象システム定義情報格納領域554に格納されている場合の表示を示している。

【0067】

図示するように、ドメイン定義画面93は、ドメインの固有情報の入力欄として、ドメイン名称、ドメインの詳細説明であるドメイン記述、および、ドメイン内の保護対象資産の入力欄932～934を有する。また、ドメイン間対応情報の入力欄として、対象ドメインとのインターフェースを有する相手ドメインを設定するための設定欄935を有する。設定欄935は、設計対象システムを構成するドメインを相手ドメイン候補として一覧表示する相手候補表示欄9351と、この相手候補表示欄9351から選択された相手ドメインを表示する相手表示欄9352とを有する。また、対象ドメインに適用する運用方針、前提条件等の運用環境を入力する入力欄936を有する。

【0068】

なお、設計対象システム定義情報格納領域554に、指定されたドメインの定義情報が格納されていない状態、つまり、これから当該ドメインの定義情報を受付ける状態では、各入力欄932～934、936および相手表示欄9352には何も表示されない。

【0069】

端末入出力装置 52 を介してユーザが各入力欄 932～934、936 に適切な情報を入力すると共に、相手ドメインを選択して相手表示欄 9352 に相手ドメインを表示させ、OK ボタン 937 を選択すると、システム構成定義 PG5421 は、各入力欄 932～934、936 および相手表示欄 9352 に表示されているドメインの固有情報、ドメイン間対応情報および運用環境情報を、当該ドメインの定義情報として、設計対象システム定義情報格納領域 554 に登録あるいは更新する（図 9 の S7112）。

【0070】

また、図 10（C）に示すように、ユーザがカーソル（不図示）を操作して表示枠 924 に表示されているサブシステムのノードを指定し、TOE 定義画面 922 において、メニューバーの項目「編集」922 から項目「定義情報の設定」9221 を選択すると、システム構成定義 PG5421 は、設計対象システム定義情報格納領域 554 に格納されている当該サブシステムの定義情報を表示すると共に当該サブシステムの定義情報の修正を受付けるためのサブシステム定義画面 94 を、端末入出力装置 52 を介して表示装置 56 に表示する。

【0071】

図 13 は、システム構成定義 PG5421 が表示装置 56 に表示するサブシステム定義画面 94 の一例を示している。この例では、図 11 において「一般利用者端末」サブシステム 9244 が指定された場合であって、「一般利用者端末」サブシステム 9244 の定義情報が既に設計対象システム定義情報格納領域 554 に格納されている場合の表示を示している。

【0072】

図示するように、サブシステム定義画面 94 は、サブシステムの固有情報の入力欄として、装置種別を示すサブシステムタイプ、サブシステム名称、サブシステムの詳細説明であるサブシステム記述、および、サブシステム内の保護対象資産の入力欄 941～934 を有する。また、サブシステム間対応情報の入力欄として、対象サブシステムとのインターフェースを有する相手サブシステムを設定するための設定欄 945 を有する。設定欄 945 は、同じドメインに属するサブシステムおよびネットワークを介して接続関係にある他ドメイン（このドメイン

は前記同じドメインのドメイン間対応情報により特定できる) のサブシステムを相手サブシステム候補として一覧表示する相手候補表示欄 9451 と、この相手候補表示欄 9451 から選択された相手サブシステムを表示する相手表示欄 9452 とを有する。また、対象サブシステムに適用する運用方針、前提条件等の運用環境を入力する入力欄 946 を有する。

【0073】

なお、設計対象システム定義情報格納領域 554 に、指定されたサブシステムの定義情報が格納されていない状態、つまり、これから当該サブシステムの定義情報を受付ける状態では、各入力欄 941～944、946 および相手表示欄 9452 には何も表示されない。

【0074】

端末入出力装置 52 を介してユーザが各入力欄 941～944、946 に適切な情報を入力すると共に、相手サブシステムを選択して相手表示欄 9452 に相手サブシステムを表示させ、OK ボタン 947 を選択すると、システム構成定義 PG5421 は、各入力欄 941～944、946 および相手表示欄 9452 に表示されているサブシステムの固有情報、サブシステム間対応情報および運用環境情報を、当該サブシステムの定義情報として、設計対象システム定義情報格納領域 554 に登録あるいは更新する (図 9 の S7114)。

【0075】

ここで、サブシステムタイプの入力欄 941 にサブシステムタイプが入力されている場合、システム構成定義 PG5421 は、このタイプを検索キーとして、システム構成事例 DB544 からサブシステムのシステム展開パターン 5441 を検索してもよい。そして、システム展開パターン 5441 を検出できたならば、検出したシステム展開パターン 5442 により特定される各コンポーネントを、対象サブシステムを構成するコンポーネントとして、図 11 に示す TOE 定義画面 92 の表示枠 924 に追加表示し、これらを対象サブシステムのノードに接続するようにしてもよい。例えば、入力欄 941 にサブシステムタイプ「IT 機器」が入力され、OK ボタン 947 が選択されると、システム構成定義 PG5421 は、サブシステムタイプ「IT 機器」のシステム展開パターン 5441 を検

索し、該パターン 5441 により特定される各コンポーネント（図 6 に示す例では、アプリケーション層、ミドルウェア層、OS 層、ハードウェア層）を、対象サブシステムを構成するコンポーネントとして設定する。そして、図 11 に示す TOE 定義画面 92 の表示枠 924 に、対象サブシステムのノードに接続された各コンポーネントのノードを追加表示する。このようにすることで、対象サブシステムを構成するコンポーネントの追加を自動化することができる。

【0076】

また、図 10 (C) に示すように、ユーザがカーソル（不図示）を操作して表示枠 924 に表示されているコンポーネントのノードを指定し、TOE 定義画面 92 において、メニューバーの項目「編集」922 から項目「定義情報の設定」9221 を選択すると、システム構成定義 PG 5421 は、設計対象システム定義情報格納領域 554 に格納されている当該コンポーネントの定義情報を表示すると共に当該コンポーネントの定義情報の修正を受付けるためのコンポーネント定義画面 95 を、端末入出力装置 52 を介して表示装置 56 に表示する。

【0077】

図 14 は、システム構成定義 PG 5421 が表示装置 56 に表示するコンポーネント定義画面 95 の一例を示している。この例では、図 11 において「勤休入力用ブラウザ」コンポーネント 9249 が指定された場合であって、「勤休入力用ブラウザ」コンポーネント 9249 の定義情報が既に設計対象システム定義情報格納領域 554 に格納されている場合の表示を示している。

【0078】

図示するように、コンポーネント定義画面 95 は、コンポーネントの固有情報の入力欄として、部品種別を示すコンポーネントタイプ、コンポーネント名称、コンポーネントの詳細説明であるコンポーネント記述、コンポーネント内の保護対象資産、コンポーネントの特徴情報（カテゴリおよびタイプ）、目標とする EAL (Evaluation Assurance Level)、および、準拠すべきセキュリティ仕様書名または使用すべき既存製品名の入力欄 951～954、958、960、961 を有する。ここで、コンポーネントの特徴情報（カテゴリおよびタイプ）は、セキュリティ仕様書事例 DB 543 からセキュリティ仕様書の事例を検索するた

めの検索キーとして用いられる。

【0079】

また、コンポーネント定義画面 95 は、コンポーネント間対応情報の入力欄として、対象コンポーネントとのインターフェースを有する相手コンポーネントを設定するための設定欄 955 と、対象コンポーネントと機能的に関係する他のコンポーネントを設定するための設定欄 959 とを有する。設定欄 955 は、同じサブシステムに属するコンポーネントおよびネットワークを介して接続関係にある他サブシステム（このサブシステムは前記同じサブシステムのサブシステム間対応情報により特定できる）に属するコンポーネントを相手コンポーネント候補として一覧表示する相手候補表示欄 9551 と、この相手候補表示欄 9551 から選択された相手コンポーネントを表示する相手表示欄 9552 と、を有する。設定欄 959 も、同様に、同じサブシステムに属するコンポーネントおよびネットワークを介して接続関係にある他サブシステムに属するコンポーネントを関連コンポーネント候補として一覧表示する関連候補表示欄 9591 と、この関連候補表示欄 9591 から選択された関連コンポーネントを表示する関連表示欄 9592 と、を有する。

【0080】

また、コンポーネント定義画面 95 は、対象コンポーネントに適用する運用方針、前提条件等の運用環境を入力する入力欄 956 を有する。なお、設計対象システム定義情報格納領域 554 に、指定されたコンポーネントの定義情報が格納されていない状態、つまり、これから当該コンポーネントの定義情報を受付ける状態では、各入力欄 951～954、956、958、960、961、相手表示欄 9552 および関連表示欄 9592 には何も表示されない。

【0081】

端末入出力装置 52 を介してユーザが各入力欄 951～954、956、958、960、961 に適切な情報を入力すると共に、相手コンポーネント、関連コンポーネントを選択して相手表示欄 9552、関連表示欄 9592 に相手コンポーネント、関連コンポーネントを表示させ、OK ボタン 957 を選択すると、システム構成定義 PG5421 は、各入力欄 951～954、956、958、

960、961、相手表示欄9552および関連表示欄9592に表示されているコンポーネントの固有情報、コンポーネント間対応情報および運用環境情報を、当該コンポーネントの定義情報として、設計対象システム定義情報格納領域554に登録あるいは更新する（図9のS7116）。

【0082】

ここで、コンポーネントタイプの入力欄951にコンポーネントタイプが入力された場合、システム構成定義PG5421は、対象コンポーネントが属するサブシステムの定義情報に含まれているサブシステムタイプを検索キーとして、運用環境事例DB545からサブシステムの運用環境パターン5451を検索し、さらに、入力欄951に入力されたコンポーネントタイプを検索キーとして、検出した運用環境パターン5451から対象コンポーネントの運用環境情報を抽出してもよい。そして、抽出した運用環境情報を、運用環境の入力欄956の初期値として表示してもよい。例えば、システム構成定義PG5421は、対象コンポーネントが属するサブシステムのタイプが「IT機器」の場合、サブシステムタイプ「IT機器」の運用環境パターン5451を検索する。そして、入力欄951にコンポーネントタイプ「アプリケーション層」が入力されると、検出した運用環境パターン5451からコンポーネントタイプ「アプリケーション層」の運用環境情報を抽出し、これを入力欄956に初期表示する。このようにすることで、対象コンポーネントの運用環境情報の作成負担を軽減することができる。

【0083】

以上のようにして、図8のS711（図9に示すフロー）が行われ、設計対象システムの定義情報が設計対象システム定義情報格納領域554に登録・更新される。

【0084】

次に、図10を用いて、図8のS712～S716（各コンポーネントのセキュリティ仕様原案の作成・登録）における操作手順と画面構成を説明する。

【0085】

図10（D）に示すように、ユーザがカーソル（不図示）を操作し、TOE定義画面92において、メニューバーの項目「ツール」923から項目「コンポー

ネット仕様書原案作成」9231を選択すると、セキュリティ仕様書選定PG5422は、設計対象システムの定義情報により特定されるコンポーネント各々を注目コンポーネントとして、図8のS712～S716を実行する。

【0086】

図15は、セキュリティ仕様書選定PG5422が表示装置56に表示する再利用可能事例画面96の一例を示している。ここで、表示枠961には、注目コンポーネントの特徴情報（カテゴリ、タイプ）958を検索キーとして、セキュリティ仕様書事例DB543から検索した既存のセキュリティ仕様書のタイトルが表示される。表示枠963には、ユーザがカーソル（不図示）を操作して表示枠961の中から選択したタイトルのセキュリティ仕様書の内容が表示される。ユーザは、表示枠963に表示されたセキュリティ仕様書の内容を参照することで、注目コンポーネントの定義情報に記載された各種情報（目標EAL、運用環境、所属サブシステム）と当該セキュリティ仕様書との整合性等を検証することができる。これにより、当該セキュリティ仕様書を注目コンポーネントに再利用できるか否かの判断を適切に行うことが可能となる。また、表示枠962は、ユーザがカーソル（不図示）を操作し、再利用するセキュリティ仕様書として、表示枠961の中から選択したタイトルのセキュリティ仕様書のタイトルが表示される。表示枠962にタイトルが表示されている状態でOKボタン964が選択されると、セキュリティ仕様書選定PG5422は、このタイトルを持つセキュリティ仕様書を、注目コンポーネントに対して再利用するセキュリティ仕様書に決定する（図8のS714）。

【0087】

図16は、セキュリティ仕様書原案作成PG5423が表示装置56に表示するセキュリティ仕様書作成・編集画面97の一例を示している。セキュリティ仕様書原案作成PG5423は、セキュリティ仕様書選定PG5422により注目コンポーネントについて再利用するセキュリティ仕様書の事例が選定されたならば、このセキュリティ仕様書の内容を、セキュリティ仕様書作成・編集画面97の注目コンポーネントのタグ971が付された編集領域972に表示する。そして、端末入出力装置52を介してユーザより、セキュリティ仕様書の編集を受付

ける。それから、ユーザより登録指示を受付けたならば、編集領域 9 7 2 に表示されているセキュリティ仕様書を注目コンポーネントのセキュリティ仕様書原案として、再利用したセキュリティ仕様書原案の情報（タイトル名など）と共に、セキュリティ仕様書原案格納領域 5 5 5 に格納する。なお、注目コンポーネントについて再利用するセキュリティ仕様書の事例が選定されなかった場合、初期状態では注目コンポーネントのタグ 9 7 1 が付された編集領域 9 7 2 に何も表示されない。したがって、ユーザは、注目コンポーネントのタグ 9 7 1 が付された編集領域 9 7 2 に、注目コンポーネントのセキュリティ仕様書原案を最初から記入する必要がある（図 8 の S 7 1 4、7 1 5）。

【 0 0 8 8 】

以上のようにして、図 8 の S 7 1 2 ～ S 7 1 6 が行われ、設計対象システムの各コンポーネントのセキュリティ仕様書原案がセキュリティ仕様書原案格納領域 5 5 5 に登録・更新される。

【 0 0 8 9 】

次に、図 1 0 を用いて、図 8 の S 7 1 7、S 7 1 8（設計対象システムのコンポジットセキュリティ仕様書原案の作成・登録）における操作手順と画面構成を説明する。

【 0 0 9 0 】

図 1 0（D）に示すように、ユーザがカーソル（不図示）を操作し、TOE 定義画面 9 2 において、メニューバーの項目「ツール」9 2 3 から項目「コンポジット仕様書原案作成」9 2 3 2 を選択すると、セキュリティ仕様書原案作成 P G 5 4 2 3 は、予め用意してあるセキュリティ仕様書の雛形に、セキュリティ仕様書原案格納領域 5 5 5 に格納されている各コンポーネントのセキュリティ仕様書原案の内容を反映させて、設計対象システムに対するコンポジットセキュリティ仕様書原案を自動作成する（図 8 の S 7 1 7）。

【 0 0 9 1 】

図 1 7 は、セキュリティ仕様書原案作成 P G 5 4 2 3 が表示装置 5 6 に表示するセキュリティ仕様書作成・編集画面 9 7 の一例を示している。図 1 7 に示すセキュリティ仕様書作成・編集画面 9 7 は、図 1 6 に示すセキュリティ仕様書作成

・編集画面 9 7 において、設計対象システムのタグ 9 7 3 が付された編集領域 9 7 4 に、セキュリティ仕様書原案作成 P G 5 4 2 3 が自動生成したコンポジットセキュリティ仕様書原案が表示されたものである。セキュリティ仕様書原案作成 P G 5 4 2 3 は、端末入出力装置 5 2 を介してユーザより、編集領域 9 7 4 に表示したコンポジットセキュリティ仕様書の編集を受付ける。それから、ユーザより登録指示を受付けたならば、編集領域 9 7 4 に表示されているコンポジットセキュリティ仕様書をセキュリティ仕様書原案格納領域 5 5 5 に格納する。これにより、セキュリティ仕様書原案格納領域 5 5 5 に、設計対象システムのシステムセキュリティ仕様書原案が登録される（図 8 の S 7 1 8）。

【0 0 9 2】

上述したように、図 1 1 は、設計対象システムの定義情報が設計対象システム定義情報格納領域 5 5 4 に格納され、また、システムセキュリティ仕様書原案がセキュリティ仕様書原案格納領域 5 5 5 に格納された状態にて、項目「TOE 定義支援」 9 1 1 1 が選択された場合に表示される TOE 定義画面 9 2 を示している。各コンポーネントのノードを、セキュリティ仕様書原案の作成に既存のセキュリティ仕様書を利用したか否かが識別できるように表示している。これは、セキュリティ仕様書原案格納領域 5 5 5 に格納されているコンポーネントのセキュリティ仕様書原案に、再利用したセキュリティ仕様書原案の情報（タイトル名など）が付されているか否かを調べることで判断することができる。既存のセキュリティ仕様書を利用したコンポーネントのノード 9 2 4 9、9 2 4 7、9 2 5 1、9 2 5 2、9 2 5 4～9 2 5 6 は、黒く塗りつぶした丸マークで表示し、既存のセキュリティ仕様書を利用していないコンポーネントのノード 9 2 4 6、9 2 4 8、9 2 5 0、9 2 5 3 は、白抜きの丸マークで表示している。このようにすることで、ユーザはコンポーネントの評価の有無を把握することができる。

【0 0 9 3】

また、図 1 1 において、サブシステムに属する全てのコンポーネントが既存のセキュリティ仕様書を利用している場合、当該サブシステムのノードを、そのことが識別できるように表示している。自身に属する全てのコンポーネントが既存のセキュリティ仕様書を利用しているサブシステム「勤休管理サーバ」のノード

9245は、黒く塗りつぶした三角マークで表示し、そうでないサブシステム「一般利用者端末」のノード9244は、白抜きの三角マークで表示している。このようにすることで、ユーザはサブシステムの評価の有無を把握することができる。ドメインも同様である。

【0094】

また、図1.1に示すTOE定義画面92において、表示枠925は、表示枠924に表示されているシステム展開ツリーから、ユーザがカーソル（不図示）を操作して選択したノードのコンポーネントが、既存のセキュリティ仕様書を再利用している場合に、その既存のセキュリティ仕様書の情報（タイトル名など）が表示される。

【0095】

以上、本発明の一実施形態について説明した。

【0096】

本実施形態によれば、設計対象システムを構成する各コンポーネントの定義情報をユーザより受付ける。次に、コンポーネント各々について、セキュリティ仕様書事例DB543に再利用可能なセキュリティ仕様書が存在するか否かを調べ、存在するならばこれを特定する。それから、予め用意してあるセキュリティ仕様書の雛形に、特定したセキュリティ仕様書各々の内容を反映して、設計対象システムに対するコンポジットセキュリティ仕様書の原案を自動生成し、ユーザに提示する。そして、ユーザよりコンポジットセキュリティ仕様書の原案の修正を受付ける。このようにすることで、専門知識・技術やノウハウをもたないユーザが設計対象システムのセキュリティ仕様書原案を作成することを支援することができる。

【0097】

本実施形態は、より具体的には以下の効果を有する。

【0098】

(1) 設計対象システムに対するコンポジットセキュリティ仕様書原案を自動生成し、差分情報のみを追加、修正することにより、セキュリティ仕様書の作成工数を削減することができる。

【0099】

(2) 各コンポーネントに対して既存（認証済み）のセキュリティ仕様書を再利用することにより、リスク分析等の専門的な技術と知識を必要とする作業を省くことができる。これにより、セキュリティ設計工数の大部分を占める分析作業を削減でき、複数の要素から構成される情報ネットワークシステムにおいて膨大となりがちな設計工数を削減できる。

【0100】

(3) 各コンポーネントに対して既存（認証済み）のセキュリティ仕様書を再利用することにより、一定品質を確保したセキュリティ仕様書原案の作成が可能となり、複数の要素から構成されるため膨大となりやすい情報ネットワークシステムの評価コストを削減できる。

【0101】

(4) システム要件等に基づいて設計対象システムを構成要素に分解、定義することができ、このため、システム構成と矛盾しないシステムセキュリティ設計が可能となる。

【0102】

(5) 顧客先でシステムセキュリティ設計コンサルテーションを行う場合等に、可搬記憶媒体に格納したセキュリティ仕様書事例DB544を利用することで、高品質なコンサルテーションサービスをすばやく提供することができる。

【0103】

なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【0104】

例えば、上記の実施形態において、セキュリティ仕様書原案作成PG5423に、コンポジットセキュリティ仕様書原案を、設計対象システムのみならず、ドメイン単位やサブシステム単位でも自動作成させるようにしてもよい。ドメインあるいはサブシステムのコンポジットセキュリティ仕様書原案の自動作成は、予め用意してあるセキュリティ仕様書の雛形に、対象ドメインあるいはサブシステムに属する各コンポーネントのセキュリティ仕様書原案の内容を反映するように

すればよい。そして、自動作成されたコンポジットセキュリティ仕様書原案をユーザに提示して修正を受付けるようにすればよい。

【0105】

また、ドメインあるいはサブシステムのコンポジットセキュリティ仕様書原案から作成したドメインあるいはサブシステムのコンポジットセキュリティ仕様書を、コンポーネントのセキュリティ仕様書と同様、セキュリティ仕様書事例DB 543に登録するようにしてもよい。サブシステムのコンポジットセキュリティ仕様書を、サブシステムタイプ（図13の入力欄941に入力される情報）、および、サブシステムを構成する各コンポーネントの特徴情報（図14の入力欄958に入力される情報）をキーとして検索できるようにデータベース化する。また、ドメインのコンポジットセキュリティ仕様書を、ドメインを構成する各サブシステムのサブシステムタイプ、および、サブシステム各々を構成する各コンポーネントの特徴情報をキーとして検索できるようにデータベース化する。

【0106】

このようにすることで、設計対象システム定義情報格納領域554に格納された設計対象システムのシステム定義情報から、ドメインあるいはサブシステムの各々について、再利用可能なドメインあるいはサブシステムのコンポジットセキュリティ仕様書の事例を検索することができる。そして、ドメインあるいはサブシステムに対して検出されたコンポジットセキュリティ仕様書を、当該ドメインあるいは当該サブシステムのコンポジットセキュリティ仕様書原案とし、当該ドメインあるいは当該サブシステム以外のドメイン、サブシステムに属する各コンポーネントのセキュリティ仕様書原案と同様に、コンポジットセキュリティ仕様書の雛形に反映させることにより、同一または類似の部分構成を備える大規模システムのセキュリティ仕様書の作成工数を削減できる。

【0107】

また、上記の実施形態において、DB543～545は、セキュリティ仕様書作成支援装置11にローカル接続されている必要はない。ネットワーク上に配置するようにしても構わない。図18は、セキュリティ仕様書作成支援装置11の変形例を示す図である。

【 0 1 0 8 】

図 1 8 に示すセキュリティ仕様書作成装置 1 1 は、例えばセキュリティ設計支援サービス企業やベンダ企業や S I (System Integrater) 企業等に設置されており、LAN、WAN等のネットワーク 1 5 を介して、セキュリティ仕様書の国際/国内登録機関や、官公庁の調達要件書を作成し管理している公的機関や、業界標準を規定する業界団体や、セキュリティ情報を提供することで利益を得ている企業等の DB 管理装置 1 5 0 と接続されている。また、DB 管理装置 1 5 0 には、セキュリティ仕様書事例 DB 5 4 3 が接続されている。

【 0 1 0 9 】

このセキュリティ仕様書作成支援装置 1 1 において、セキュリティ仕様書選定 P G 5 4 2 2 は、ネットワーク I F 装置 5 8 および DB 管理装置 1 5 0 を介して、セキュリティ仕様書事例 DB 5 4 3 にアクセスし、再利用可能なセキュリティ仕様書の事例を入手する。このようにすることで、ネットワーク 1 5 上に分散する多種多様な既存のセキュリティ仕様書の中から設計対象に最適なものを効率的に選定したり、官公庁や業界団体が指定する最新のセキュリティ仕様書を直接入手したりすることが可能となり、より高品質かつ効率的な設計が可能となる。

【 0 1 1 0 】**【発明の効果】**

以上説明したように、本発明によれば、複数の I T 製品で構成される情報ネットワークシステムに対するセキュリティ仕様書の作成を支援することができる。

【図面の簡単な説明】**【図 1】**

図 1 は、本発明の一実施形態が適用されたセキュリティ仕様書作成支援装置 1 1 により、設計対象システム 1 6 に対するコンポジットセキュリティ仕様書原案が作成されるまでの大まかな処理の流れ（原理）を示す図である。

【図 2】

図 2 は、設計対象システムの一例を示す図である。

【図 3】

図 3 (A) は国際セキュリティ評価基準 I S O 1 5 4 0 8 準拠セキュリティ仕

様書（P P / S T）の構成例 3 1 および各種定義情報の記述例 3 3 を示す図であり、図 3（B）はコンポジットセキュリティ仕様書の一例 3 5 を示す図である。

【図 4】

図 4 は、本実施形態のセキュリティ仕様書作成支援装置 1 1 の概略図である。

【図 5】

図 5 は、セキュリティ仕様書事例 D B 5 4 3 のデータ管理の仕組みを説明するための図である。

【図 6】

図 6 は、システム構成事例 D B 5 4 4 の登録例を示す図である。

【図 7】

図 7 は、運用環境事例 D B 5 4 5 の登録例を示す図である。

【図 8】

図 8 は、本実施形態のセキュリティ仕様書作成支援装置 1 1 の動作フローを説明するための図である。

【図 9】

図 9 は、図 8 の S 7 1 1 での処理（設計対象システムの定義情報の受付・登録）の詳細なフローを示す図である。

【図 1 0】

図 1 0（A）～図 1 0（D）は、システム構成定義 P G 5 4 2 1 が表示装置 5 6 に表示する作業画面のメニューバーの一例を示す図である。

【図 1 1】

図 1 1 は、システム構成定義 P G 5 4 2 1 が表示装置 5 6 に表示する T O E 定義画面 9 2 の一例を示す図である。

【図 1 2】

図 1 2 は、システム構成定義 P G 5 4 2 1 が表示装置 5 6 に表示するドメイン定義画面 9 3 の一例を示す図である。

【図 1 3】

図 1 3 は、システム構成定義 P G 5 4 2 1 が表示装置 5 6 に表示するサブシステム定義画面 9 4 の一例を示す図である。

【図 14】

図 14 は、システム構成定義 P G 5 4 2 1 が表示装置 5 6 に表示するコンポーネント定義画面 9 5 の一例を示す図である。

【図 15】

図 15 は、セキュリティ仕様書選定 P G 5 4 2 2 が表示装置 5 6 に表示する再利用可能事例画面 9 6 の一例を示す図である。

【図 16】

図 16 は、セキュリティ仕様書原案作成 P G 5 4 2 3 が表示装置 5 6 に表示するセキュリティ仕様書作成・編集画面 9 7 の一例を示す図である。

【図 17】

図 17 は、セキュリティ仕様書原案作成 P G 5 4 2 3 が表示装置 5 6 に表示するセキュリティ仕様書作成・編集画面 9 7 の一例を示す図である。

【図 18】

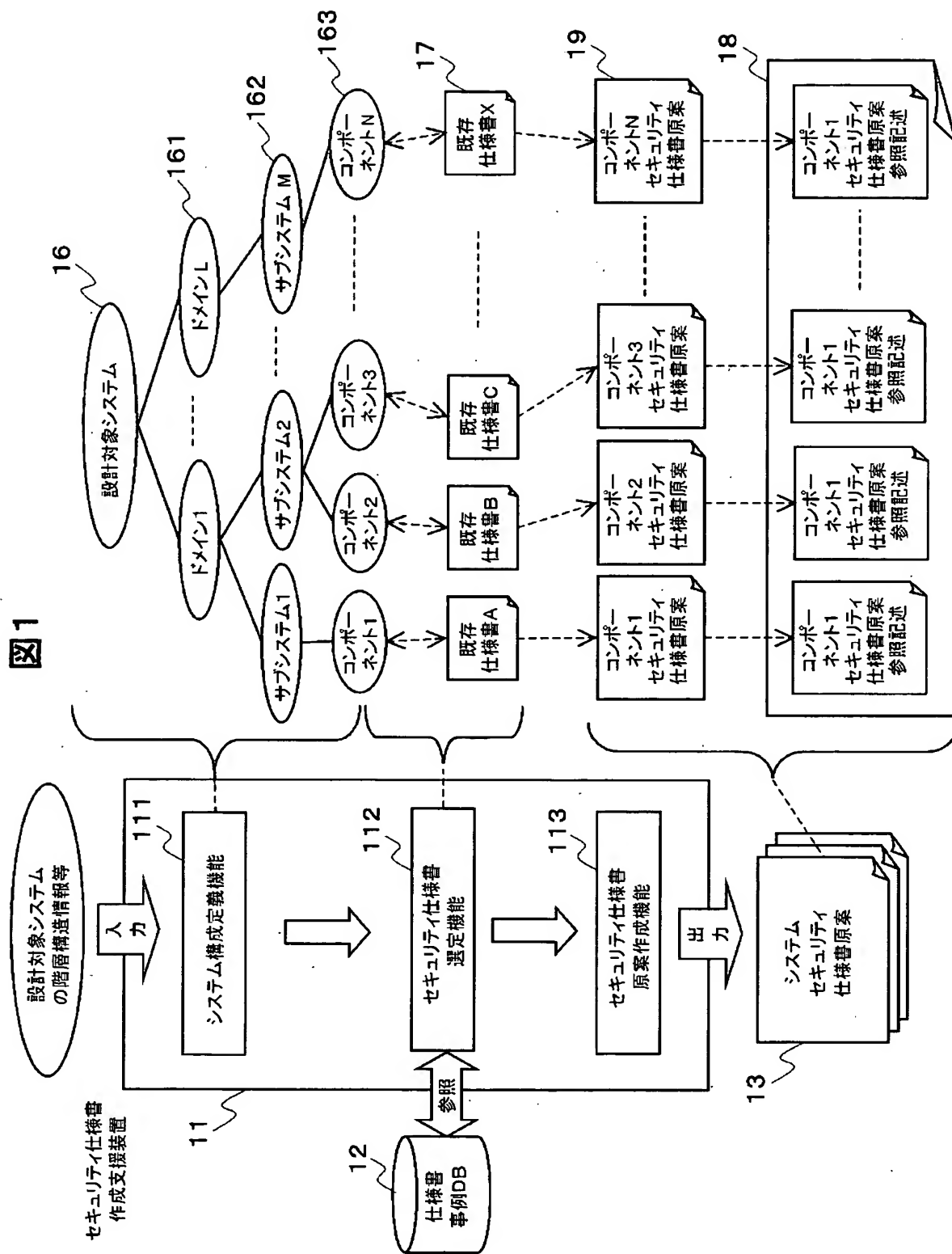
図 18 は、セキュリティ仕様書作成支援装置 1 1 の変形例を示す図である。

【符号の説明】

1 1 …セキュリティ設計支援装置、5 1 …CPU、5 2 …端末入出力装置、5 3 …バス、5 4 …外部記憶装置、5 5 …メモリ、5 6 …表示装置、5 7 …入力装置、5 8 …ネットワーク I F 装置、5 9 …可搬記憶媒体入出力装置、5 4 1 …通信制御 P G、5 4 2 …セキュリティ仕様書作成支援 P G、5 4 3 …セキュリティ仕様書事例 D B、5 4 4 …システム構成事例 D B、5 4 5 …運用環境事例 D B、5 5 1 …運用環境事例格納領域、5 5 2 …システム構成事例格納領域、5 5 3 …セキュリティ仕様書事例格納領域、5 5 4 …設計対象システム定義情報格納領域、5 5 5 …セキュリティ仕様書原案格納領域、5 9 1 …可搬記憶媒体、5 4 2 1 …システム構成定義 P G、5 4 2 2 …セキュリティ仕様書選定 P G、5 4 2 3 …セキュリティ仕様書原案作成 P G

【書類名】 図面

【図 1】



【図 2】

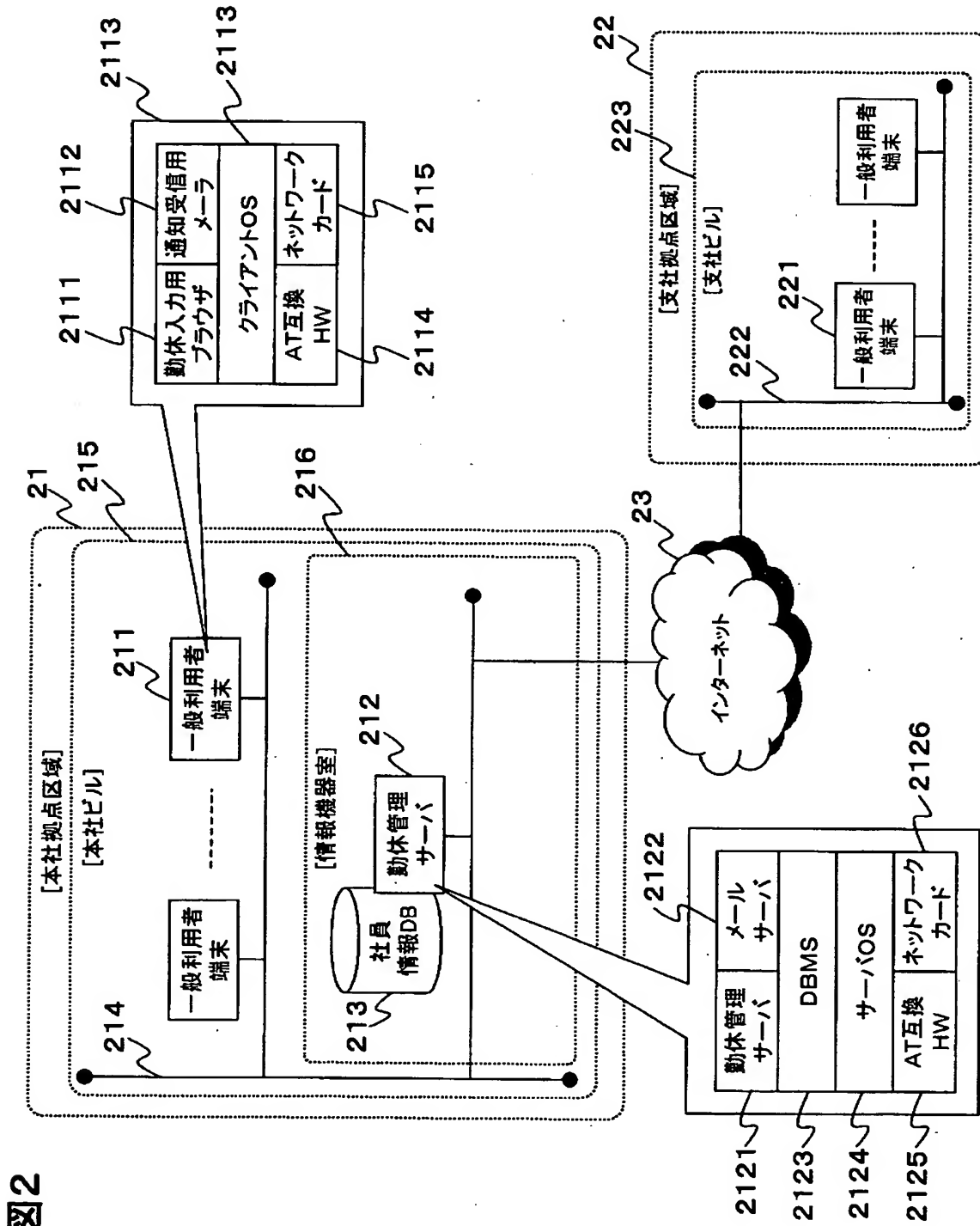


図2

【図3】

(B) コンポジットセキュリティ仕様書

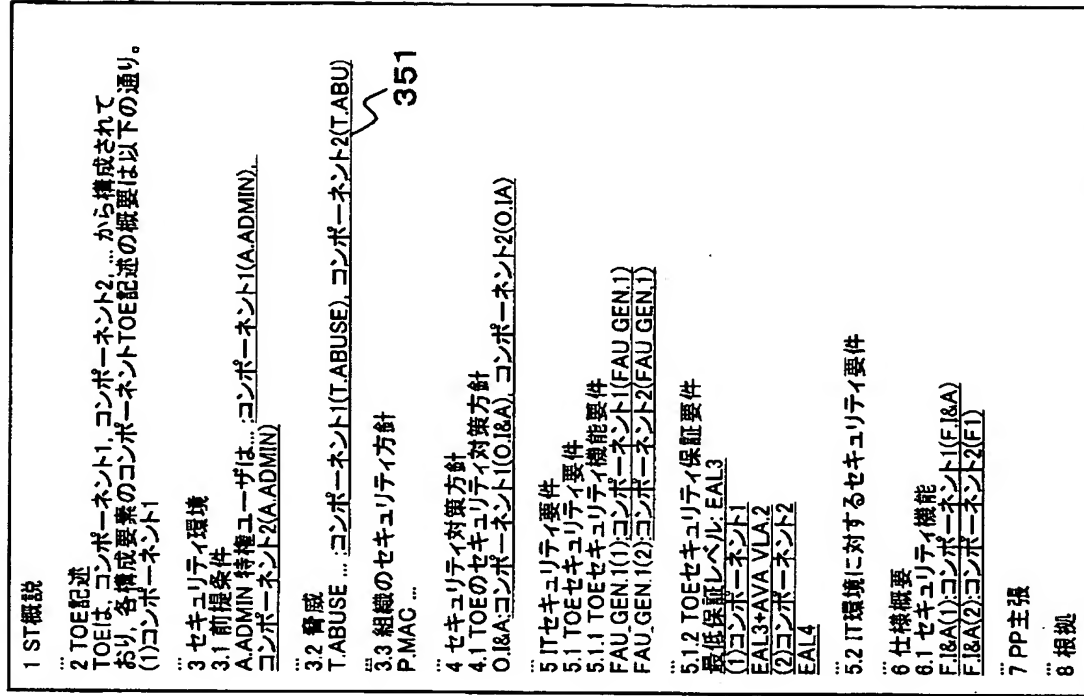
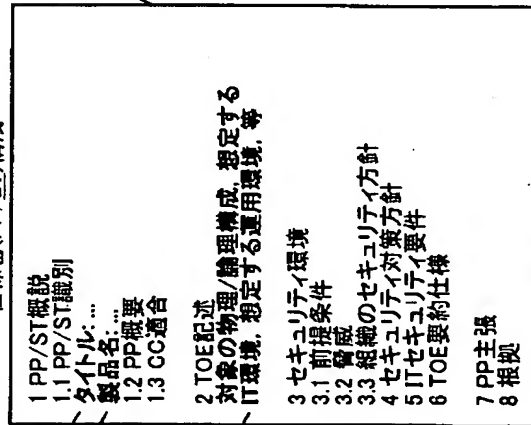


図3

(A) ISO15408準拠セキュリティ仕様書(PP/ST)構成



各種定義情報の記述

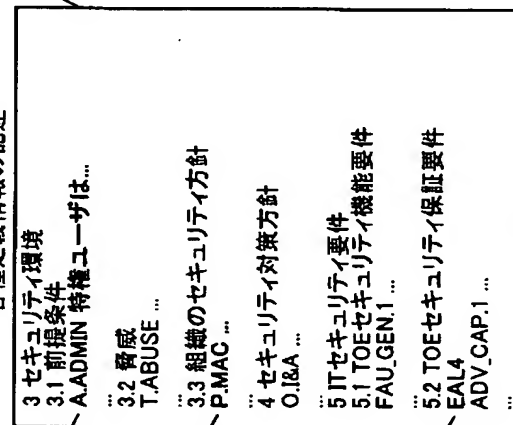
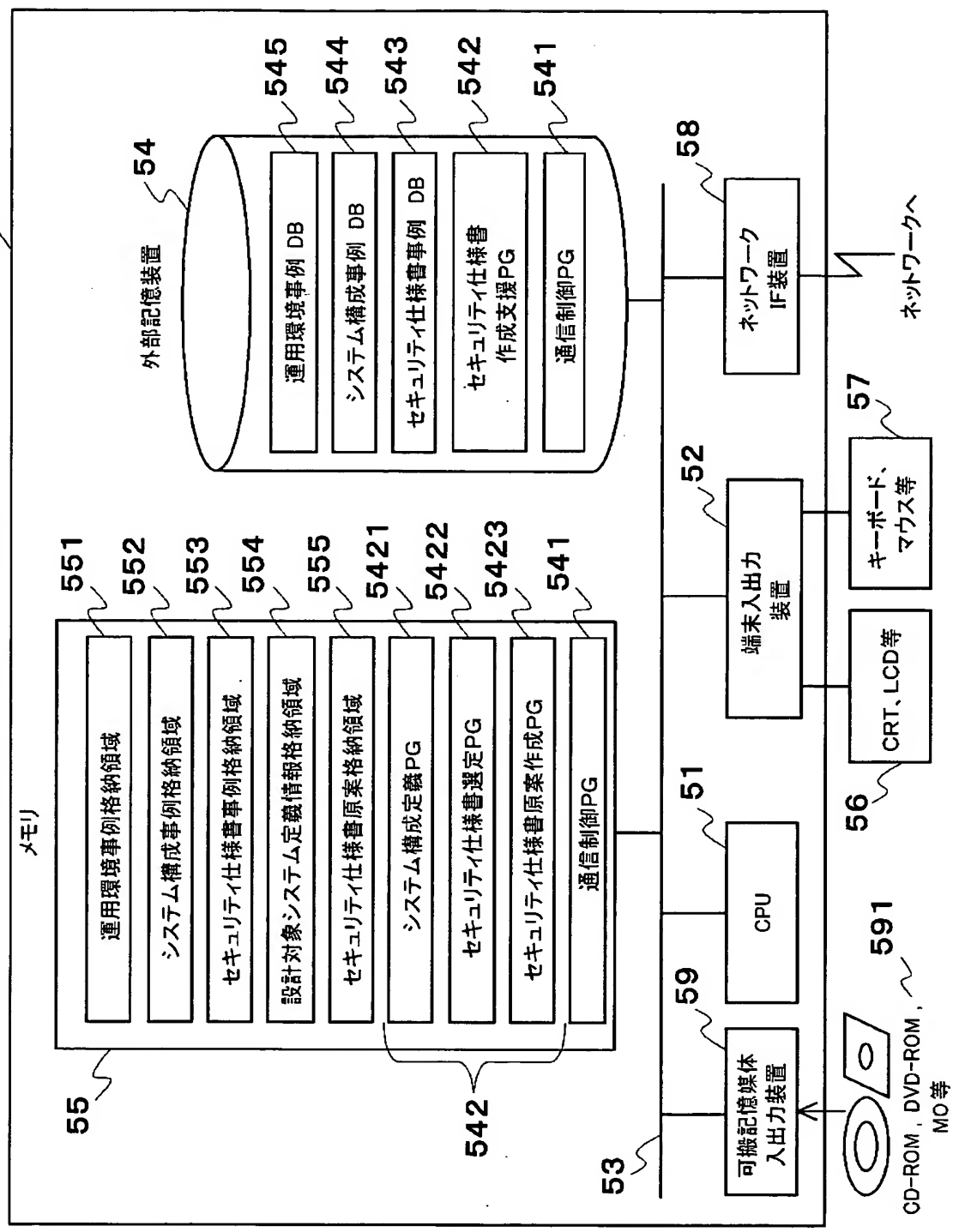


図4

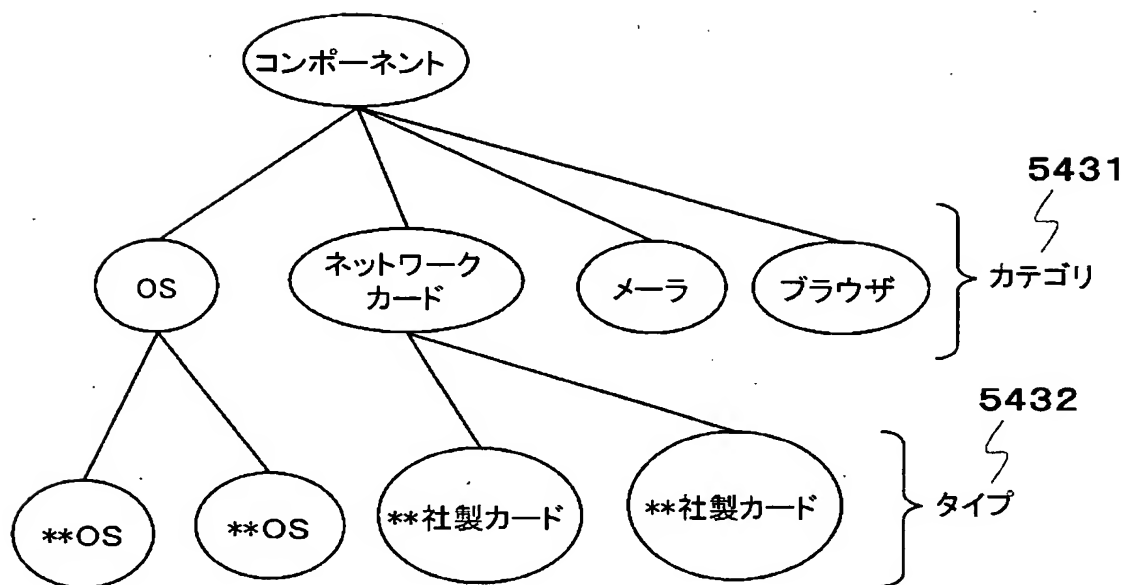
【図4】

セキュリティ仕様書作成支援装置



【図 5】

図5

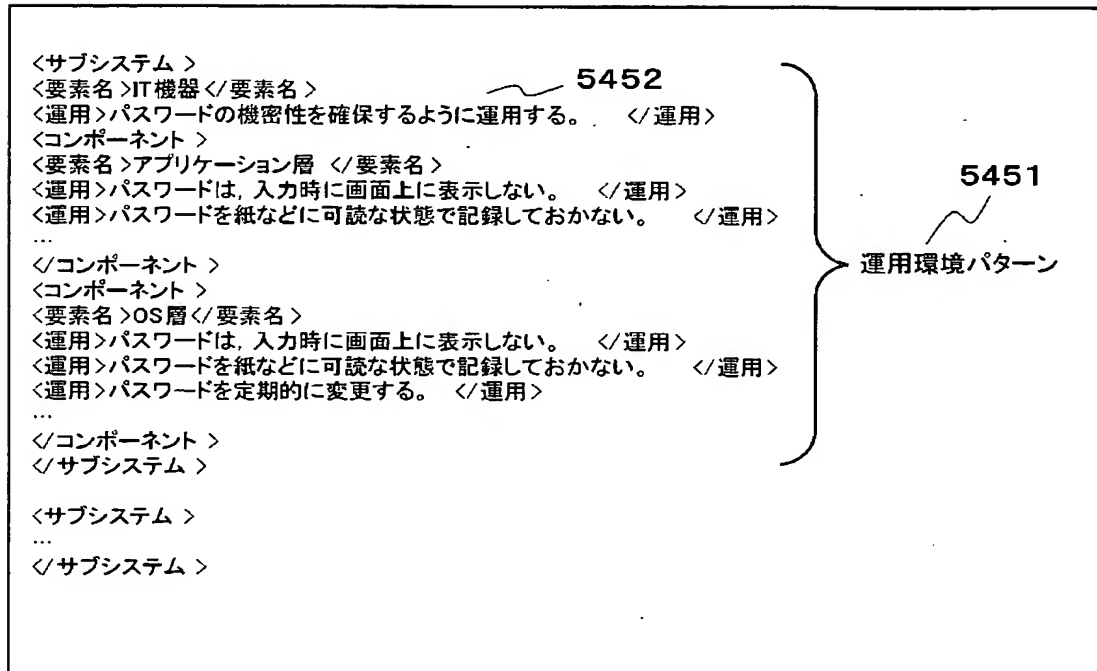


セキュリティ仕様書事例DB543

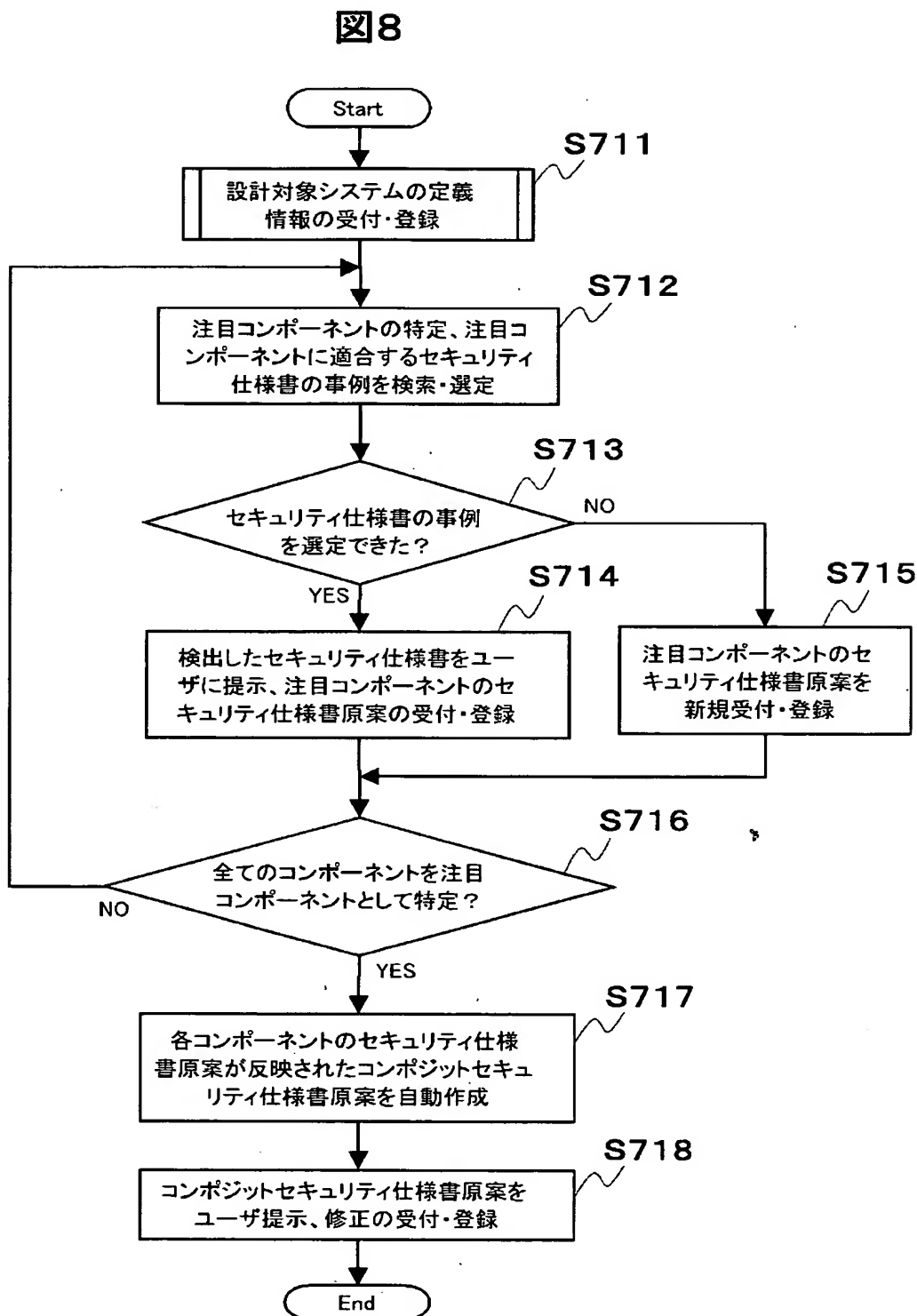
【図 7】

図 7

運用環境事例 DB545

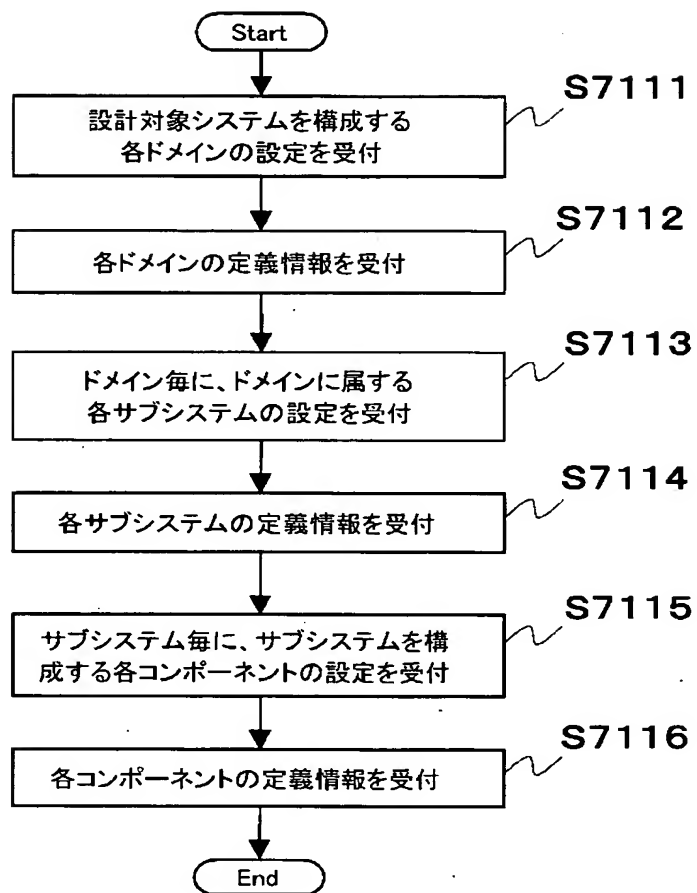


【図 8】



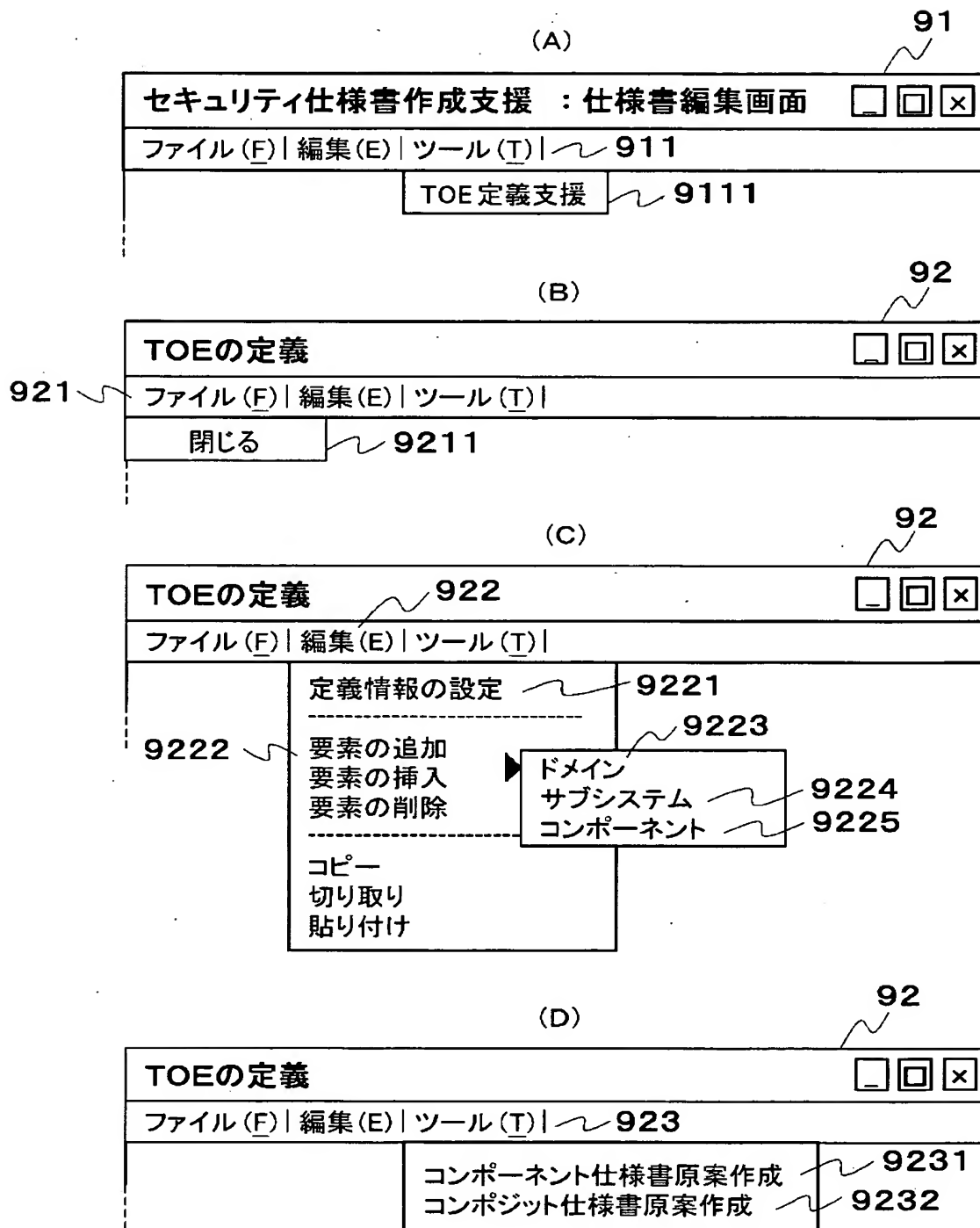
【図 9】

図 9



【図10】

図10



【図 11】

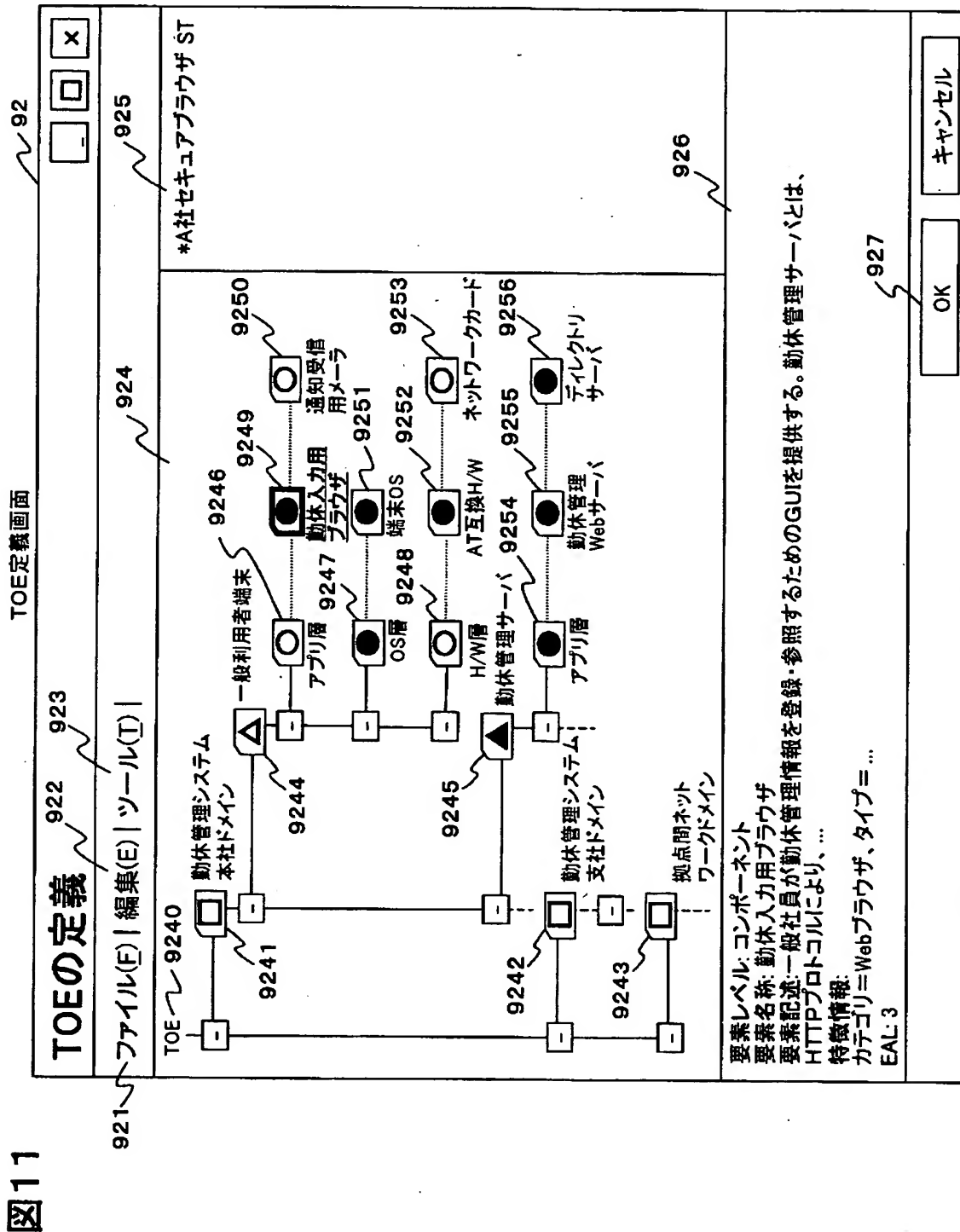


図12

【図12】

ドメイン定義画面

932 ドメイン名称

933 ドメイン記述

934 資産名称

935 I/Fありドメイン

936 運用環境

937 OK キャンセル

93 ドメイン定義 - TOE: 勤休管理システム

本社拠点区域

本社ビル内に設置されているサブシステムのグループであり、...

機密情報

ドメイン間 I/F のある相手ドメイン候補

追加>>

<<削除

9352

ドメイン間 I/F のある相手ドメイン

拠点間ネットワーク

暗号通信を行う。

図13

サブシステム定義画面

94

【図13】

サブシステム定義 - ドメイン: 本社拠点区域

941

サブシステム
タイプ

IT機器

ICカード

H社ICカード

942

サブシステム
名称

一般利用者端末(本社)

943

サブシステム
記述

一般利用者が本社ビル内から勤体管理サーバにアクセスする際に使用するクラ
イアント端末。この端末の使用に際しては、...

944

資産名称

社員個人情報

945

V/Fありドメイン

9451

サブシステム間 V/Fのある相手サブシステム候補

勤体管理サーバ

本社ネットワーク

拠点間ネットワーク

支社ネットワーク

一般利用者端末(支社)

9452

サブシステム間 V/Fのある相手サブシステム

追加>>

<<削除

本社ネットワーク

946

運用環境

パスワードの機密性を確保するように運用する。

一定時間経過後に業務用ソフトウェアを終了し、端末からログオフする。

947

OK

キャンセル

【図 14】

図14

コンポーネント定義画面

コンポーネント定義 - サブシステム: 一般利用ユーザー端末

951 コンポーネントタイプ アプリケーション層

952 コンポーネント名称 勤休入力用ブラウザ

953 コンポーネント記述 一般社員が勤休管理情報を登録・参照するためのGUIを提供する。勤休管理サーバとは、HTTPプロトコルにより、...

954 資産名称 "社員勤休情報"、"ユーザID"、"パスワード"

955 I/Fあり
コンポーネント 9551
コンポーネント間 I/Fのある相手コンポーネント候補
通知受信用メーラ
端末 OS
追加>> <<削除

959 関連
コンポーネント 9591
コンポーネント間 I/Fのある相手コンポーネント候補
通知受信用メーラ
端末 OS
追加>> <<削除

956 運用環境

958 コンポーネント特徴

960 EAL

コンポーネント間 I/Fのある相手コンポーネント
端末 OS
9552

関連するコンポーネント
端末 OS
勤休管理サーバ
9592

パスワードは、入力時に画面上に表示しない。
パスワードを紙などに可読な状態で記録しておくかない。
利用者 IDを複数のユーザで共有しない。

特徴種別毎に特徴情報を設定して下さい。

カテゴリ Webブラウザ ▼ タイプ ▼

3 ▼ 指定の仕様書・製品

957 OK 961 キャンセル

【図 1 5】

図15

再利用率事例選択画面

96

再利用率事例選択 - 注目コンポーネント: ネットワークカード

再利用率事例

962

Smart card Integrated Circuit PP v0.9

961

追加>>

<<削除

検出されたセキュリティ仕様書事例

Smart card Integrated Circuit PP v0.9

Smart card Operating System PP v1.2

H社 ICカード Security Target ver. 1.1

Smart Card Embedded Software ST ver. 2.0

963

タイトル: Smart Card Integrated Circuit Protection Profile

バージョン: 0.9 (draft)

作成日: Jan 1, 2003

作成者: Smart Card Vender Group

登録名: SCIC-PP

...

概要:

This PP describes the IT security requirements for a smart card to ...

964

OK

キャンセル

【図 16】

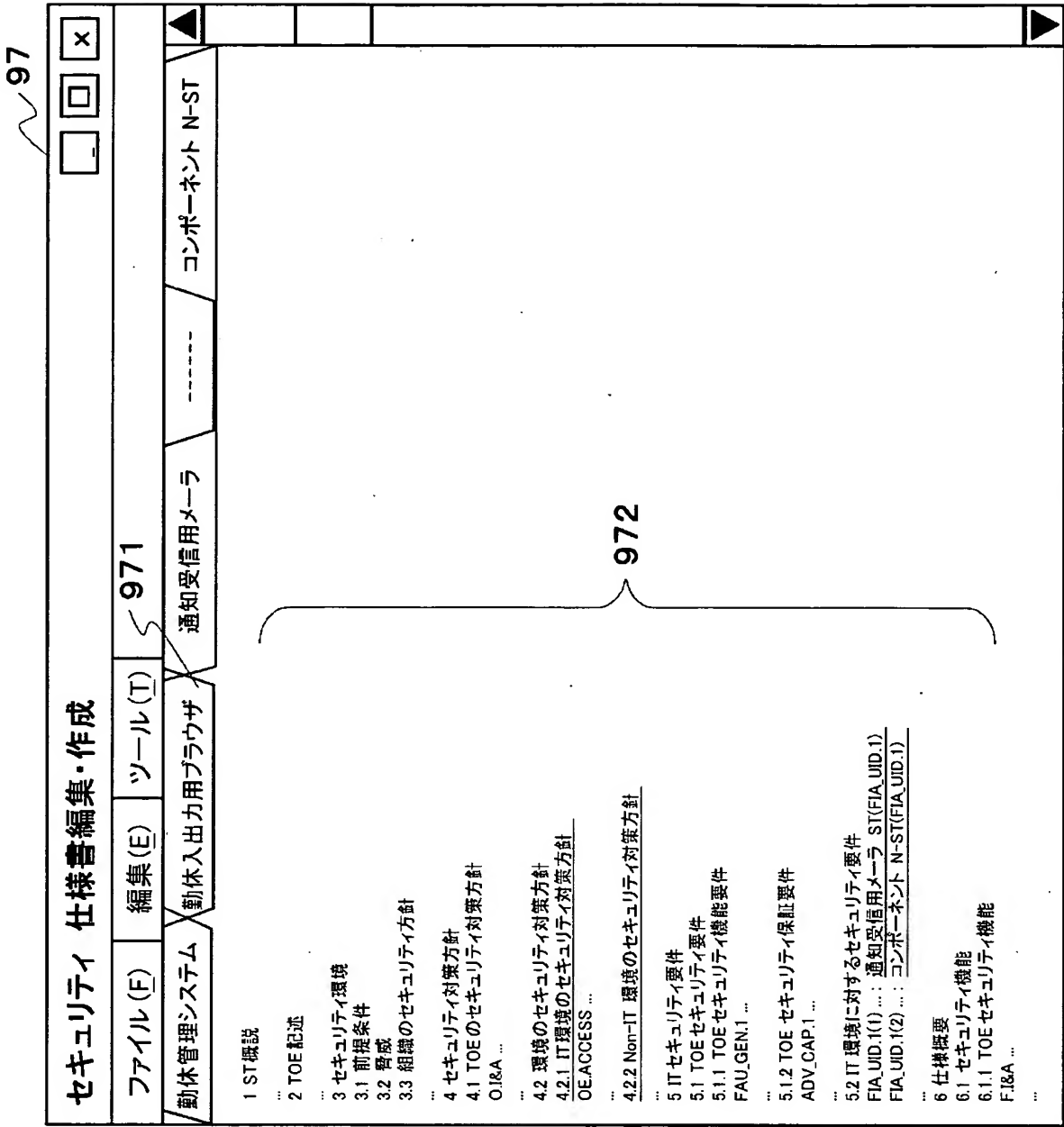


図16

【図 17】

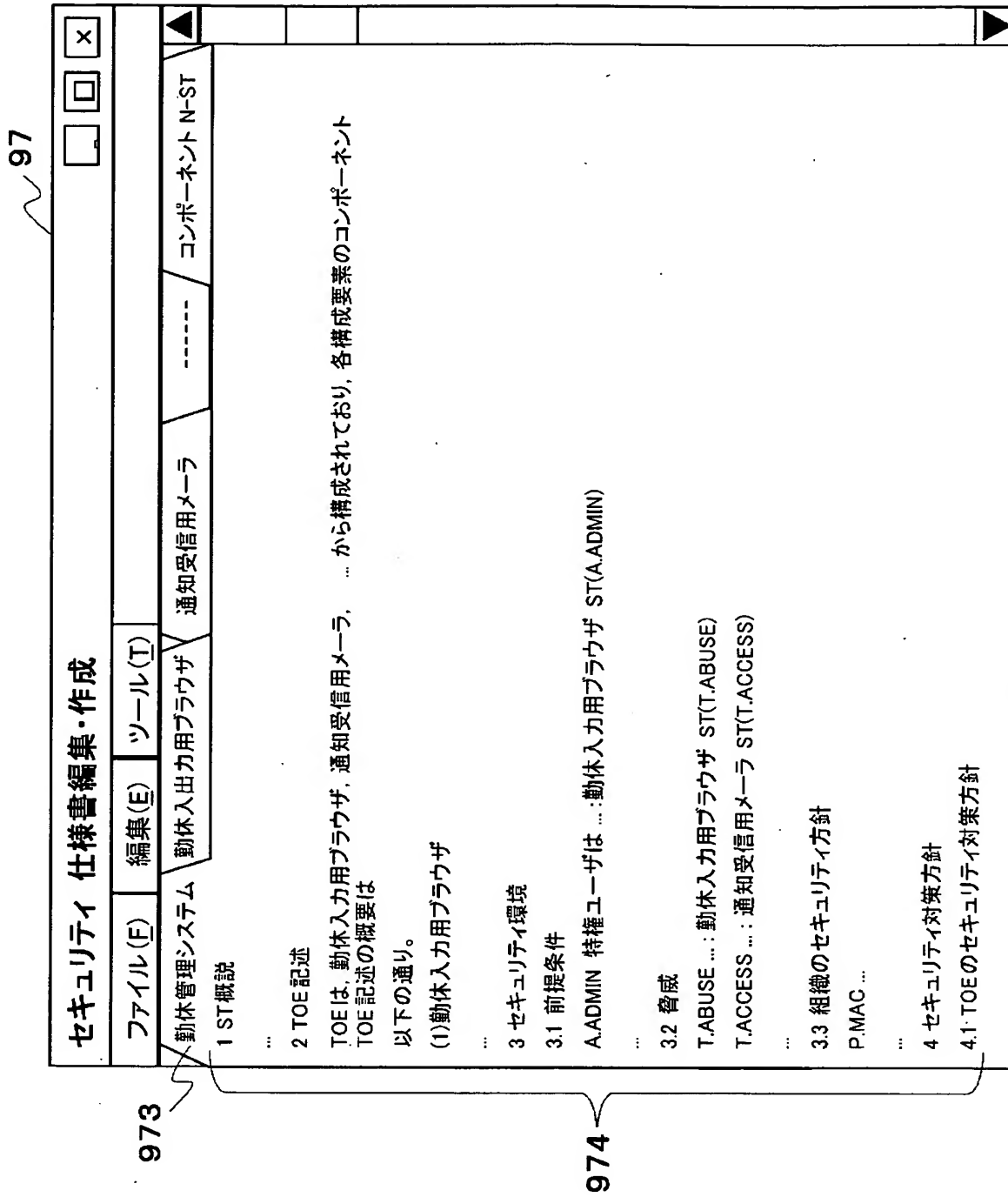
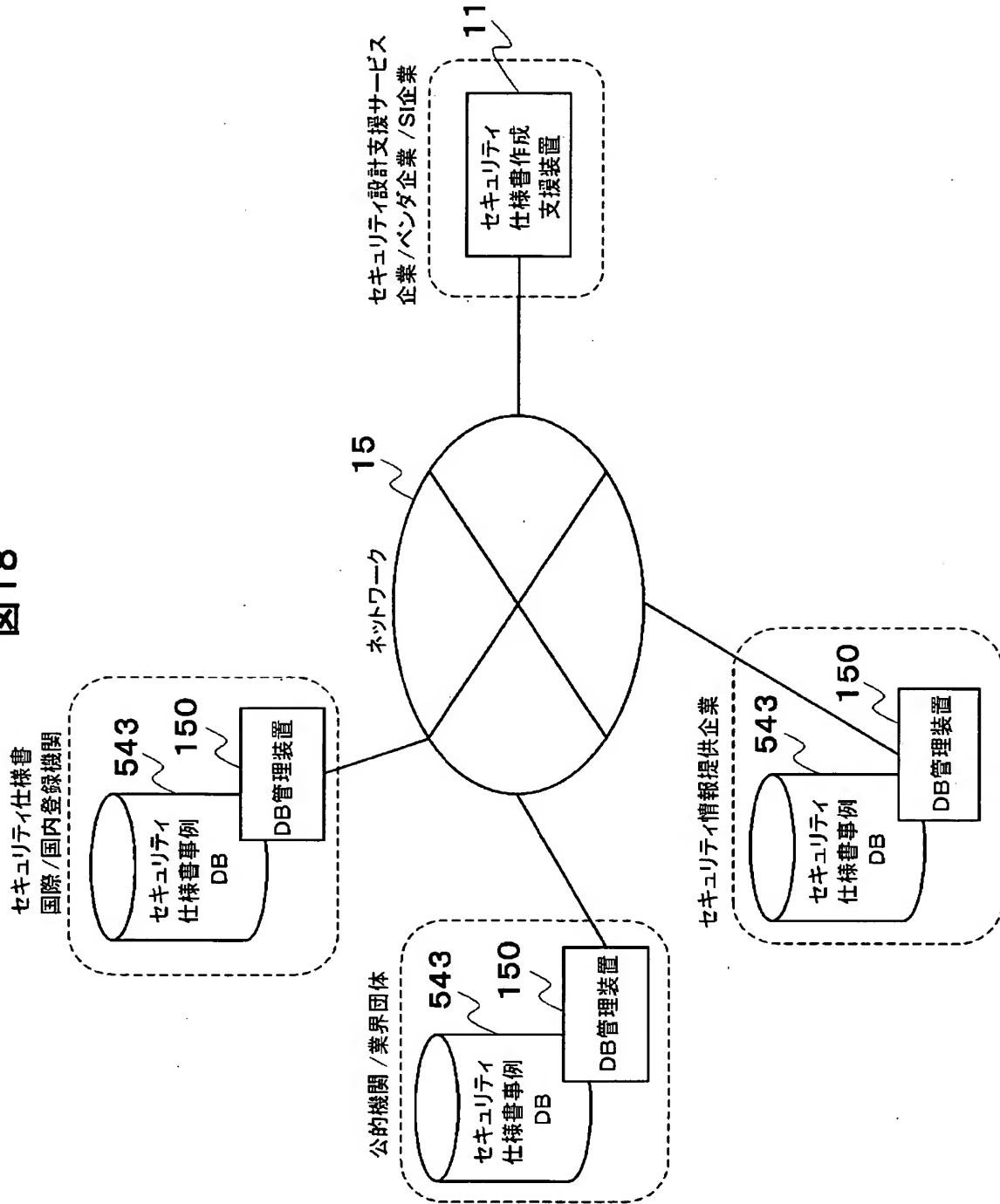


図17

【図 18】

図 18



【書類名】 要約書**【要約】**

【課題】複数のIT製品で構成される情報ネットワークシステムに対するセキュリティ仕様書の作成を支援する。

【解決手段】セキュリティ仕様書作成支援装置11において、システム構成定義PG5421は、設計対象システムを構成する各コンポーネントの定義情報をユーザより受付ける。セキュリティ仕様書選定PG5422は、コンポーネント各々について、セキュリティ仕様書事例DB543に再利用可能なセキュリティ仕様書が存在するか否かを調べ、存在するならばこれを特定する。そして、セキュリティ仕様書原案作成PG5423は、予め用意してあるセキュリティ仕様書の雛形に、特定したセキュリティ仕様書各々の内容を反映して、設計対象システムに対するコンポジットセキュリティ仕様書の原案を自動生成する。

【選択図】 図4

特願 2003-134706

出願人履歴情報

識別番号

[000005108]

1. 変更年月日

1990年 8月31日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台4丁目6番地

氏 名

株式会社日立製作所